МИНОБРНАУКИ РОССИИ
ФЕДЕРАЛЬ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ
«ВОРОНЕЖСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ»
БОРИСОГЛЕБСКИЙ ФИЛИАЛ
(БФ ФГБОУ ВО «ВГУ»)

МЕТОДИЧЕСКИЕ МАТЕРИАЛЫ ПО УЧЕБНОЙ ДИСЦИПЛИНЕ
Элементы абстрактной и компьютерной алгебры

Методические указания для обучающихся по освоению дисциплины

Приступая к изучению учебной дисциплины, целесообразно ознакомиться с учебной программой дисциплины, электронный вариант которой размещён на сайте БФ ВГУ.

Это позволит обучающимся получить четкое представление о:

- перечне и содержании компетенций, на формирование которых направлена дисциплина;
- основных целях и задачах дисциплины;
- планируемых результатах, представленных в виде знаний, умений и навыков, которые должны быть сформированы в процессе изучения дисциплины;
- количестве часов, предусмотренных учебным планом на изучение дисциплины, форму промежуточной аттестации;
- количестве часов, отведенных на контактную и на самостоятельную работу;
- формах контактной и самостоятельной работы;
- структуре дисциплины, основных разделах и темах;
- системе оценивания учебных достижений;
- учебно-методическом и информационном обеспечении дисциплины.

Знание основных положений, отраженных в рабочей программе дисциплины, поможет обучающимся ориентироваться в изучаемом курсе, осознавать место и роль изучаемой дисциплины в подготовке будущего выпускника, строить свою работу в соответствии с требованиями, заложенными в программе.

Основными формами контактной работы по дисциплине являются лекции и практические занятия, посещение которых обязательно для всех студентов (кроме студентов, обучающихся по индивидуальному плану).

Подготовка к практическим занятиям ведется на основе планов практических занятий. В ходе подготовки к практическим занятиям необходимо изучить в соответствии с вопросами для повторения конспекты лекций, основную литературу, ознакомиться с дополнительной литературой. Кроме того, следует повторить материал лекций, ответить на контрольные вопросы, изучить образцы решения задач, выполнить упражнения (если такие предусмотрены).

При подготовке к промежуточной аттестации необходимо повторить пройденный материал в соответствии с учебной программой, примерным перечнем вопросов, выносящихся на экзамен. Рекомендуется использовать конспекты лекций и источники, перечисленные в списке литературы в рабочей программе дисциплины, а также ресурсы электронно-библиотечных систем.

Методические материалы для обучающихся по освоению теоретических вопросов дисциплины

Тема1. Алгебраические системы

План

1. *Отношения эквивалентности. Отношения порядка.*
2. *Связь отношений эквивалентности с разбиениями множества.*
3. *Понятие и свойства бинарной алгебраической операции.*
4. *Группы. Нормальные делители. Конечные группы.*
5. *Кольца и поля.*

1. Отношения эквивалентности. Отношения порядка

ОПРЕДЕЛЕНИЕ. *Декартовым произведением* множеств A и B называется множество, состоящее из всех упорядоченных пар элементов вида <a, b>, в которых первый элемент принадлежит первому множеству, а второй – второму.

Обозначение: $A \times B = \{\langle a, b\rangle / a \in A, b \in B\}$.

Если множества A и B совпадают, то декартово произведение называют также *декартовым квадратом* множества A: $A \times A = A^2$.

ОПРЕДЕЛЕНИЕ. *Бинарным отношением,* заданным на непустом множестве A, называется всякое подмножество декартова квадрата множества A.

Для обозначения бинарных отношений используют либо специальные значки, общепринятые, например: =, ≤ , ≥ , ∥ , ⊥ и т.д., либо буквы греческого алфавита: α, δ, σ, φ, ρ и т.д.

Если элементы *x* и *y* множества A находятся в некотором бинарном отношении *σ,* то это может обозначаться одним из следующих образов:

$\langle x, y\rangle \in \sigma$, либо $x \sigma y$.

ОПРЕДЕЛЕНИЕ. Бинарное отношение ρ, заданное на непустом множестве A, называется:

- *рефлексивным,* если $(\forall a \in A)$ справедливо $\langle a, a\rangle \in \rho$;
- *антирефлексивным,* если $(\forall a \in A)$ справедливо $\langle a, a\rangle \notin \rho$;
- *симметричным,* если $(\forall a, b \in A)$ из того, что пара $\langle a, b\rangle \in \rho$, следует, что пара $\langle b, a\rangle \in \rho$;
- *транзитивным,* если для $(\forall a, b, c \in A)$, из того, что пара $\langle a, b\rangle \in \rho$ и пара $\langle b, c\rangle \in \rho$, следует, что пара $\langle a, c\rangle \in \rho$;
- *антисимметричным,* если для любых различных элементов $a, b \in A$ из того, что $\langle a, b\rangle \in \rho$ и $\langle b, a\rangle \in \rho$ следует, что $a = b$;
- *асимметричным,* если $(\forall a, b \in A, a \neq b)$ условие $\langle a, b\rangle \in \rho$ никогда не влечет за собой выполнение условия $\langle b, a\rangle \in \rho$;
- *отношением эквивалентности,* если оно рефлексивно, симметрично и транзитивно одновременно;
- *отношением порядка,* если оно антисимметрично и транзитивно;

Если при этом отношение *ρ* обладает свойством антирефлексивности, то оно называется отношением *строгого порядка,* если же *ρ* обладает свойством рефлексивности, то – отношением *нестрогого порядка.*

ОПРЕДЕЛЕНИЕ. Отношение порядка ρ, заданное на множестве A, называется *отношением линейного порядка,* если для любых двух элементов $a, b \in A$ выполняется одно и только одно из условий:

$a = b$ или $\langle a, b\rangle \in \rho$ или $\langle b, a\rangle \in \rho$.

Говорят также, что в этом случае отношение ρ обладает свойством *связности.*

Если бинарное отношение ρ задано на конечном множестве, то его наглядно можно изобразить с помощью *ориентированного графа.* При этом элементы самого множества изображаются точками на плоскости.

Если пара $\langle a, b\rangle \in \rho$, то соответствующие точки соединяются ориентированным ребром от a к b.

Также можно построить *график* бинарного отношения. Для этого по осям абсцисс и ординат откладываются элементы множества, а на координатной плоскости строятся точки, координаты которых соответствуют элементам бинарного отношения.

Верно и обратное. Любой ориентированный граф, а также график можно рассматривать как граф или график бинарного отношения и определять по ним его свойства.

ПРИМЕР **1**. Пусть A = {1, 2, 4, 6}.

Тогда декартов квадрат множества A будет равен:

A×A = {<1, 1>; <2, 2>; <4, 4>; <6, 6>; <1, 2>; <2, 1>; <1, 4>; <4, 1>;
<1, 6>; <6, 1>; <2, 4>; <4, 2>; <2, 6>; <6, 2>; <4, 6>; <6, 2>}.

Следующее подмножество ρ множества A×A является, согласно определению, бинарным отношением, заданным на множестве A:

ρ = {<2, 2>; <4, 4>; <1, 2>; <2, 1>; <1, 4>; <6, 2>; <4, 6>}.

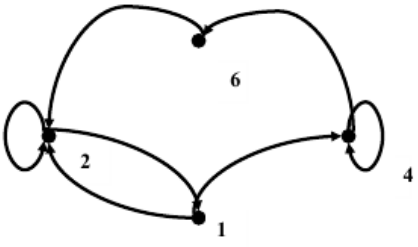
Данное отношение не обладает свойством рефлексивности, так как, например, пара <1, 1> ему не принадлежит.

С другой стороны, оно не обладает и свойством антирефлексивности, поскольку оно содержит пары <2, 2> и <4, 4>.

Отношение ρ не симметрично, хотя бы уже потому, что оно содержит пару <1, 4>, но не содержит пары <4, 1>. Однако, оно не будет также являться ни антисимметричным, ни асимметричным, поскольку ему одновременно принадлежат пары элементов <1, 2> и <2, 1>, причем $2 \neq 1$.

Отношение ρ не обладает также свойством транзитивности, так как, хотя пары <1, 4> и <4, 6> ему принадлежат, пара <1, 6> отношению ρ не принадлежит.

Построим граф и график этого бинарного отношения:



Граф отношения ρ

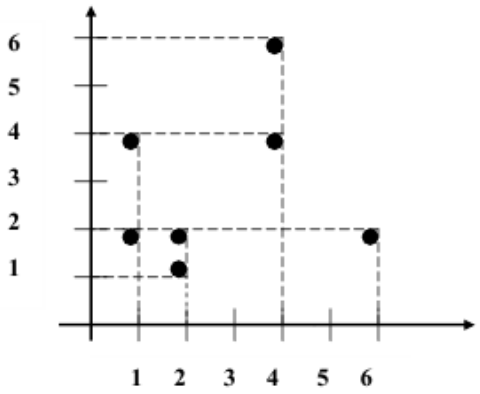


График отношения ρ

ЗАМЕЧАНИЯ. 1. Из определений следует, что ни одно бинарное отношение не может обладать одновременно свойствами рефлексивности и антирефлексивности или свойствами симметричности и антисимметричности (асимметричности). В то же время из примера следует, что некоторые бинарные отношения могут вообще не обладать ни одним из свойств соответствующей пары.

2. Примерами отношения эквивалентности могут служить:

- отношение равенства « = » на любом числовом множестве;
- отношение параллельности « ∥ » на множестве всех прямых плоскости;
- отношение ρ на множестве всех слов русского алфавита, если два слова *u* и *v* находятся в отношении ρ тогда и только тогда, когда они начинаются с одной и той же буквы, поскольку каждое из этих отношений, очевидно, обладает свойствами рефлексивности, симметричности и транзитивности.

3. Примерами отношения порядка могут служить:

- отношения сравнения по величине « < » и « > » на множестве целых чисел;
- отношение делимости нацело « **:** » на множестве натуральных чисел.

При этом первые два отношения есть отношения строгого линейного порядка, поскольку они обладают свойством антирефлексивности и связности (ни одно целое число не может быть строго больше или меньше самого себя и из двух различных целых чисел одно обязательно больше либо меньше другого), а последнее – нестрогого нелинейного порядка, так как оно, напротив, рефлексивно и несвязно (каждое натуральное число делится само на себя и для двух различных натуральных чисел не обязательно одно делится на другое нацело).

2. Связь отношений эквивалентности с разбиениями множества

ОПРЕДЕЛЕНИЕ. Говорят, что набор подмножеств множества A образует *разбиение* этого множества, если выполняются следующие условия:

1) хотя бы одно из подмножеств непусто,

2) никакие два подмножества не пересекаются,

3) объединение всех подмножеств совпадает с множеством A.

Подмножества называются в этом случае *классами разбиения.*

Множество $\bar{A}$, элементами которого являются классы данного разбиения, называют *фактор-множеством* множества A по данному разбиению.

Существует самая тесная связь между разбиениями некоторого множества и отношениями эквивалентности, которые можно на данном множестве построить.

ТЕОРЕМА. *По каждому отношению эквивалентности, заданному на множестве A, можно построить некоторое разбиение этого множества. И обратно, каждому разбиению множества A соответствует некоторое отношение эквивалентности.*

ЗАМЕЧАНИЯ

1. Следствием этой теоремы, которое имеет практическое значение, является тот факт, что существует взаимно-однозначное соответствие между множеством всех различных разбиений множества A и множеством всех различных отношений эквивалентности, которые можно задать на этом множестве. Таким образом, различных отношений эквивалентности на данном множестве будет ровно «столько», «сколько» различных разбиений этого множества можно построить.

2. Пусть дано разбиение множества A и соответствующее ему отношение эквивалентности ρ. Тогда фактор-множество по данному разбиению называют также фактор-множеством по отношению эквивалентности *ρ* и обозначают A/ρ .

ПРИМЕР **2**.

1. Пусть дано множество A = {a, b, c, d} и отношение эквивалентности на нем:

ρ = {<a, a>; <d, d>; <a, d>; <d, a>; <c, c>; <b, b>}.

Чтобы построить по отношению ρ разбиение этого множества, достаточно в один класс разбиения поместить те и только те элементы множества A, которые находятся в отношении ρ:

A = {a, d}; A = {c}; A = {b}.

2. Пусть дано множество A = {a, b, c, d}, на котором задано разбиение:

A = {a}; A = {b, c}; A = {d}.

Чтобы построить по данному разбиению соответствующее ему отношение эквивалентности, достаточно отнести к этому отношению те и только те пары элементов, которые принадлежат одному классу разбиения: ρ = {<a, a>; <b, b>; <c, c>; <.b, c>; <c, b>; <d, d>}.

ПРИМЕР **3.** Зададим на множестве Z отношение ≡ по следующему правилу:

$$b \equiv a \pmod m \Rightarrow b - a = m \cdot q,\ q, m \in Z,\ m > (1).$$

Говорят, что *a сравнимо с b по модулю m*.

Очевидно, что это отношение есть отношение эквивалентности, так как оно рефлексивно, симметрично и транзитивно. Также очевидно, что числа a и b сравнимы по mod m тогда и только тогда, когда они дают при делении на m одинаковые остатки.

Классами разбиения по данному отношению ≡ являются множества вида:

{a+m·q | q - целое} = {…,-3m+a, -2m+a, -m+a, a, m+a, 2m+a, 3m+a,…},

которые обозначаются через a+mZ или просто $\bar{a}$ и называются *классами вычетов* или просто *вычетами*.

Фактор-множество Z/ ≡ обозначается обычно через Z_m и называется *множеством вычетов или множеством целых чисел по модулю m*.

ЗАМЕЧАНИЕ. Каждый класс разбиения по отношению ≡ содержит бесконечно много элементов. Само множество классов эквивалентности содержит ровно *m*

элементов. Обычно из каждого класса эквивалентности выбирают представителя – неотрицательное число, которое при делении на *m* дает остаток r, где $0 \le r < m$.

3. Понятие и свойства бинарной алгебраической операции

Отображения* или *функции

ОПРЕДЕЛЕНИЕ. Бинарное отношение f, заданное на паре множеств A и B, называется *отображением* или *функцией* из A в B, если выполняются условия:

1) для любого элемента $a \in A$ найдется такой элемент $b \in B$, что пара $<a, b> \in f$;

2) для любого элемента $a \in A$ и любых элементов $b, c \in B$ из того, что пары $<a, b>$ и $<a, c>$ одновременно принадлежат отношению f, следует, что $b = c$.

Если пара $<a, b>$ принадлежит отношению f, то первый элемент пары называют *прообразом* второго, а второй – *образом* первого.

ЗАМЕЧАНИЕ. Учитывая последнее, определение короче можно сформулировать следующим образом:

Бинарное отношение f, заданное на паре множеств A и B, называется *отображением* или *функцией* из A в B, если каждый элемент множества A имеет *единственный* образ в множестве B.

Обозначение. Если f есть отображение из A в B и пара $<a, b> \in f$, то это записывают как $f(a) = b$.

ОПРЕДЕЛЕНИЕ. Отображение f из A в B называется *инъективным (или инъекцией)*, если для любых элементов $a, b \in A$ выполняется условие:

$$f(a) = f(b) \Rightarrow a = b.$$

Отображение f из A в B называется *сюръективным (или сюръекцией, или отображением «на»)*, если для всякого элемента $b \in B$ найдется такой элемент $a \in A$, для которого $f(a) = b$ (каждый образ имеет прообраз в множестве A).

Отображение f из A на B называется *биективным (или биекцией или взаимно-однозначным*, если оно инъективно и сюръективно одновременно.

ПРИМЕР **1**.

1. Пусть $f = \{<x, y> \in R^{+} \times R \,/\, x = y^2\}$. Данное отношение отображением не является, так как не выполнено второе условие из определения 8. Например, для $x = 4$ имеем $y = \sqrt{4} = 2$ и $y_1 = -\sqrt{4} = -2$. Таким образом, пары $<4, 2>$ и $<4, -2>$ одновременно принадлежат отношению f, хотя $2 \ne -2$.

2. Пусть $f = \{<x, y> \in R \times R \,/\, x^2 = y\}$. Очевидно, что в этом случае каждое действительное число x имеет единственный образ в множестве R, и потому f является отображением.

Однако из того, что $f(2) = f(-2) = 4$, не следует, что $2 = -2$, потому f не инъективно.

Кроме того, если $y < 0$, то нельзя найти ни одного элемента $x \in R$, для которого выполнялось бы равенство $x^2 = y$. Следовательно, отображение f не сюръективно.

3. Пусть $f = \{<x, y> \in R \times R \,/\, y = 2x\}$. Очевидно, что в этом случае f также является отображением. Более того, так как для любых действительных чисел x и x_1:

$$f(x) = f(x_1) \Leftrightarrow 2x = 2x_1 \Leftrightarrow x = x_1,$$

то отображение f инъективно, а так как для любого действительного числа y существует такое число $x = \frac{y}{2}$, что:

$$f(x) = f\left(\frac{y}{2}\right) = 2 * \frac{y}{2} = y,$$

то отображение f сюръективно. Следовательно, f является биекцией.

ОПРЕДЕЛЕНИЕ. Пусть f - отображение из множества X в множество Y:

$$f = \{<x, y> \,/\, x \in X, y \in Y\}.$$

Соответствие f^{-1} = {<y, x> / где <x, y> $\in$ f} называется *обратным* к отображению f.

ТЕОРЕМА. Соответствие f^{-1}, обратное к отображению f, само является отображением тогда и только тогда, когда отображение f биективно.

ОПРЕДЕЛЕНИЕ. *Бинарной алгебраической операцией*, заданной на множестве A, называется отображение f: A × A → A, которое каждой паре элементов из множества *A* ставит в соответствие некоторый элемент этого же множества:

$$(\forall a,b \in A)\ (\exists c \in A)\ f\text{: } \langle a, b\rangle \to c$$

Обозначение: a f b = c. Для обозначения бинарных операций обычно используют не буквы, а специальные значки: « +», « * »,«-», « : », « ◦ » и т.д.

ЗАМЕЧАНИЕ

Подобное определение можно сформулировать для n-арной алгебраической операции при любом конечном натуральном n. Однако в абстрактной алгебре наиболее часто, кроме бинарной, используют понятия унарной и нульарной операций.

ОПРЕДЕЛЕНИЕ. *Унарной алгебраической операцией*, заданной на множестве A, называется отображение f: A → A, которое каждому элементу множества A ставит в соответствие некоторый элемент этого же множества:

$$(\forall a \in A)\ (\exists c \in A)\text{: } f(a) = c.$$

Нульарной алгебраической операцией, заданной на множестве A, называется выделение в этом множестве некоторого фиксированного элемента.

ОПРЕДЕЛЕНИЕ. Операция « * », заданная на непустом множестве A, называется:

- *ассоциативной,* если:

$$(\forall a, b, c \in A)\ a * (b * c) = (a * b) * c;$$

- *коммутативной,* если:

$$(\forall a, b \in A)\ a * b = b * a.$$

ОПРЕДЕЛЕНИЕ. Говорят, что операция « * », заданная на непустом множестве A, обладает:

- *левым [правым] нейтральным элементом,* если:

$$(\exists e \in A)\ (\forall a \in A)\ \ e * a = a\ [a * e = a];$$

- *двусторонним нейтральным элементом (*или просто *нейтральным),* если она обладает и левым и правым нейтральным элементами, причем эти элементы совпадают:

$$(\exists e \in A)(\forall a \in A)\ \ e * a = a * e = a.$$

ОПРЕДЕЛЕНИЕ

Операция « * », заданная на непустом множестве A, называется:

- *обратимой слева [справа],* если:

$$(\forall a \in A)\ (\exists b \in A)\ b * a = e,\ [a * b = e],$$

где *e* – левый [правый] нейтральный элемент множества *A* по операции « * ».

- *двусторонне обратимой* (или просто *обратимой*), если она обратима и справа и слева:

$$(\forall a \in A)\ (\exists b \in A)\ a * b = b * a = e,$$

где *e* – нейтральный элемент множества A по операции *« * ».*

- *сократимой слева [справа],* если:

$$(\forall a, b, c \in A)\ (c * a = c * b \Rightarrow a = b).$$
$$[a * c = b * c \Rightarrow a = b].$$

- *сократимой,* если она сократима и слева и справа.

ОПРЕДЕЛЕНИЕ. Пусть на множестве A заданы две бинарные алгебраические операции - «* » и « ◦ ».

Операция « ◦ » называется *дистрибутивной слева [справа]* относительно операции « * », если:

$$(\forall a, b, c \in A)\ c \circ (a * b) = (c \circ a) * (c \circ b)$$
$$[(a * b) \circ c = (a \circ c) * (b \circ c)].$$

Операция « ◦ » называется *дистрибутивной* относительно операции « * », если она дистрибутивна относительно данной операции и слева и справа.

ЗАМЕЧАНИЯ

1. При проверке свойств бинарной операции, заданной на некотором множестве, прежде всего необходимо проверить, является ли данная операция алгебраической на данном множестве. Так, например, операция вычитания не является алгебраической на множестве N натуральных чисел, так как для случая, когда a < b, результат этой операции a – b < 0 и, следовательно, не принадлежит множеству N.

2. Очевидно, что не все свойства операций независимы друг от друга. Так, если по данной операции в данном множестве нет нейтрального элемента, то не имеет смысла говорить и об обратимости этой операции.

3. Если операция « * » коммутативна на множестве A, то любое из свойств, которое выполняется для нее слева или справа, очевидно, будет выполняться и с другой стороны.

4. Группы. Нормальные делители. Конечные группы

группы играют в современной абстрактной алгебре настолько важную роль и их приложения имеют настолько широкий спектр, что изучение различных классов групп, групповых конструкций и их свойств выросло в самостоятельную научную теорию – теорию групп. Поэтому в алгебре чаще используются несколько отличные от приведенного выше определения группы через так называемые групповые аксиомы.

ОПРЕДЕЛЕНИЕ 1. *Группой* называется алгебраическая структура **G** = < G, * , $^{-1}$, e >, где G ≠ ∅ - основное множество структуры, на котором заданы:

- одна бинарная алгебраическая операция « * »;
- одна унарная алгебраическая операция $^{-1}$;
- одна нульарная алгебраическая операция – выделение нейтрального элемента *e*, удовлетворяющие следующим аксиомам:

1) операция « * » ассоциативна: $(\forall a, b, c \in G)\ a*(b*c) = (a*b)*c$;

2) по данной операции существует нейтральный элемент:
$$(\exists e \in G)\ (\forall a \in G)\ \ e*a = a*e = a;$$

3) операция « * » обратима на м G*:*
$$(\forall a \in G)\ (\exists b \in G)\ \ a*b = b*a = e.$$

ОПРЕДЕЛЕНИЕ 2. *Группой* называется алгебраическая структура **G** = < G, * >, где G – непустое основное множество структуры, « * » - бинарная алгебраическая операция, заданная на G, причем выполняются следующие аксиомы:

1) операция *« * »* ассоциативна: $(\forall a, b, c \in G)\ a*(b*c) = (a*b)*c$;

2) $(\forall a, b \in G)\ (\exists x, y \in G)\ \ a*x = b$ и $y*a = b$ (т.е. в группе разрешимы уравнения такого вида).

ТЕОРЕМА. Определения 1 и 2 группы эквивалентны, то есть, если алгебраическая структура с одной бинарной операцией является группой в смысле определения 1, то она является группой и в смысле определения 2, и обратно.

ЗАМЕЧАНИЯ

1. Так как в определении группы отсутствует требование коммутативности бинарной операции, то в определении 1 необходимо требовать существования решения обоих уравнений, поскольку из разрешимости уравнения a*x = b в этом случае не следует разрешимость уравнения y*a = b и наоборот. Если же операция в группе коммутативна, то группу называют *абелевой.*

2. Чаще всего операцию в группе обозначают символами « + » или « • » и называют *сложением* и *умножением* соответственно. В первом случае группа называется *аддитивной,* нейтральный элемент – *нулем,* обратный элемент – *противоположным* и обозначаются они как 0 и -a. Во втором случае группу называют *мультипликативной.*

3. *Натуральной степенью* элемента g мультипликативной группы < G, • > называется элемент g^n = g • g • … • g (n раз), n ∈ N;

Степенью с отрицательным показателем называется элемент

$$g^{-n} = g^{-1} \bullet g^{-1} \bullet \ldots \bullet g^{-1} \text{ (n раз), } n \in N.$$

4. Если группа конечна, то число ее элементов называется *порядком* группы. В противном случае группа называется группой *бесконечного порядка.*

Обозначение: порядок группы G обозначается как $|G|$.

5. Часто группа обозначается одной буквой G без указания операции.

ПРИМЕРЫ

1**.** Аддитивными абелевыми группами являются, например, структуры:

$$< Z, + >, < Q,, + >, < R, + >,$$

где Z, Q и R - множества целых, рациональных и действительных чисел соответственно.

2. Примерами мультипликативных абелевых групп могут служить структуры: $< Q^*, \bullet >$, $< R^*, \bullet >$, где Q^* и R^* - множества всех ненулевых рациональных и действительных чисел соответственно.

3. Примером некоммутативной группы может служить множество всех квадратных невырожденных матриц порядка *n* по операции матричного умножения.

4. Наибольший теоретический и прикладной интерес представляет группа симметрий правильного n-угольника, называемая *диэдрической группой Dn* или *группой диэдра.*

Элементами Dn являются, во-первых, n поворотов вокруг центра многоугольника на углы $\varphi_k = k \cdot \frac{2\pi}{n}$, где k = 0, 1, ..., (n - 1), во-вторых, n осевых симметрий. Осями симметрии служат: в случае четного n - n/2 диагоналей, соединяющих противоположные вершины, и (n/2) прямых, соединяющих середины противоположных сторон; в случае нечетного n - n высот многоугольника (рис. 3). Других симметрий у многоугольника нет.

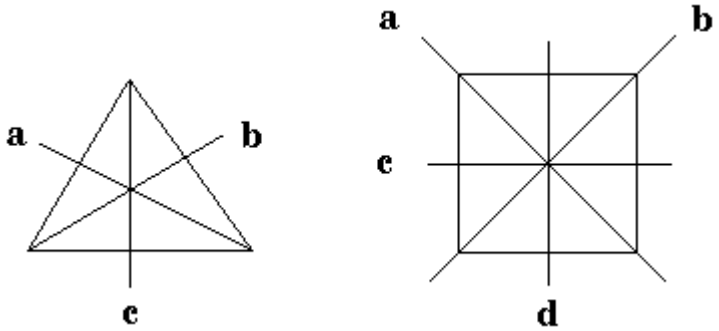


Рис. 3. Оси симметрий правильных многоугольников

Используя группы симметрий, Е. С. Федоров в 1890 году решил задачу классификации правильных пространственных систем точек, являющуюся одной из основных задач кристаллографии. Существует всего 17 плоских федоровских групп, они были найдены непосредственно; пространственных федоровских групп - 230, и только теория групп позволила провести их исчерпывающую классификацию. Это был исторически первый случай применения теории групп непосредственно в естествознании.

Следующая теорема выражает простейшие свойства групп.

ТЕОРЕМА. Во всякой группе < G, ·> выполняются следующие свойства:

1) В G существует и притом единственный нейтральный элемент.

2) Для всякого элемента a группы G существует и притом единственный обратный элемент a^{-1}.

3) Для любых элементов a и b группы G справедливы равенства:

$$(a^{-1})^{-1} = a \text{ и } (a \cdot b)^{-1} = b^{-1} \cdot a^{-1}.$$

4) В группе < G, ·> нет делителей нуля.

5) В группе G уравнения a*x = b и y*a = b однозначно разрешимы для любых элементов a и b.

6) Во всякой группе операция двусторонне сократима.

ОПРЕДЕЛЕНИЕ. Подмножество H группы < G, ·> называется ее *подгруппой*, если оно само является группой относительно операции «·», определенной в группе G.

ТЕОРЕМА (*критерий подгруппы*). Подмножество H группы < G, ·> является ее подгруппой тогда и только тогда, когда выполняется условие:

$$(\forall a, b \in H) \quad a \cdot b^{-1} \in H.$$

ЗАМЕЧАНИЕ. Говорят, что подмножество H группы < G, ·> является ее подгруппой, если оно *замкнуто* относительно операции, определенной в группе G, и относительно операции взятия обратного элемента.

ПРИМЕРЫ.

1. Подгруппами всякой группы < G, · > являются сама эта группа и единичная подгруппа E, состоящая только из одного нейтрального элемента группы G : E = { e }. Эти подгруппы называются *несобственными.* Всякая подгруппа группы *G,* отличная от этих двух, называется *собственной.*

2. Множество всех четных чисел является подгруппой аддитивной группы всех целых чисел < Z, + >, так как для любых четных чисел a и b число a + (-b) является четным.

3. Множество {-1, 1} образует подгруппу мультипликативной группы всех ненулевых действительных чисел < R, · >.

4**.** Совокупность <g> = $\{g^n / n \in Z\}$ степеней элемента g группы G является подгруппой в G.

Отметим некоторые простейшие свойства подгрупп.

СВОЙСТВО **1.** Пересечение произвольной совокупности подгрупп группы *G* само будет подгруппой этой группы.

СВОЙСТВО **2.** Объединение двух подгрупп группы G будет являться подгруппой в том и только в том случае, когда одна из них содержится в другой.

ОПРЕДЕЛЕНИЕ. Подгруппа <g> = $\{g^n / n \in Z\}$ группы G называется *циклической подгруппой, порожденной элементом g.*

ЗАМЕЧАНИЕ. Если в группе принята аддитивная форма записи операции, то степени элемента g группы G называются *кратными* и обозначаются ng, ($n \in Z$).

ТЕОРЕМА **2.** Подгруппа <g> группы G конечна в том и только в том случае, когда

$$(\exists n \in N)\ g^n = e.$$

ЗАМЕЧАНИЕ. Если n – минимальное число со свойством $g^n = e$, то оно называется *порядком элемента g.* Если же $(\forall n \in N)\ g^n \neq e$, то все степени элемента g будут различны между собой, и подгруппу <g> называют *бесконечной циклической,* и сам элемент g – *элементом бесконечного порядка.*

Нормальные делители. Фактор-группы

ОПРЕДЕЛЕНИЕ. Пусть H – подгруппа группы < G, •>, g – произвольный элемент группы G. Множество H • g [g • H] всех элементов группы G, которые представимы в виде h • g [g • h], где h пробегает множество элементов подгруппы H, т. е.

$$H \bullet g = \{h \bullet g / h \in H\}$$

$$[\ g \bullet H = \{g \bullet h / h \in H\}\ ]$$

называется *правым [левым] смежным классом* группы G по подгруппе H.

ТЕОРЕМА. Пусть дана группа < G, •>, в ней подгруппа H и g – произвольный элемент из G. Тогда выполняются следующие свойства:

1) если элемент a принадлежит правому смежному классу H • g, то

$$H \bullet a = H \bullet g,$$

т.е. всякий правый смежный класс группы G по подгруппе H задается любым из своих элементов, который называется *представителем класса* $H \bullet g$;

2) два любых смежных класса группы G по подгруппе H либо не пересекаются, либо совпадают;

3) одним из правых смежных классов группы G по подгруппе H является сама подгруппа H, и других подгрупп среди правых смежных классов группы G по подгруппе H нет;

4) объединение всех правых смежных классов группы G по подгруппе H совпадает с самой группой G.

СЛЕДСТВИЕ.

Множество всех правых классов группы G по подгруппе H образует разбиение этой группы, которое называют *правосторонним разложением* группы G по подгруппе H:

$$G = h_1 \bullet g \cup h_2 \bullet g \cup \ldots \cup h_\delta \bullet g \quad (h_i \in H).$$

ЗАМЕЧАНИЯ

1. Аналогичные свойства можно сформулировать и для левых смежных классов. Соответствующее разбиение называют *левосторонним разложением* группы G по подгруппе *H.* Эти оба разложения состоят из одного и того же числа смежных классов. Если это число конечно, то оно называется *индексом* подгруппы H в группе G.

2. Пусть G – конечная группа порядка n, H – ее подгруппа порядка n и индекса k. Тогда из следствия предыдущей теоремы получаем равенство: $n = m \bullet k$.

ТЕОРЕМА *Лагранжа.*

1. Порядок и индекс любой подгруппы конечной группы являются делителями порядка самой группы.

2. Порядок любого элемента конечной группы является делителем порядка группы.

ОПРЕДЕЛЕНИЕ. Подгруппа H группы G называется *нормальной подгруппой* или *нормальным делителем* группы G, если для любого элемента $g \in G$ левый и правый смежные классы по подгруппе H совпадают:

$$(\forall\, g \in G)\ \ H \bullet g = g \bullet H.$$

В этом случае говорят просто о *разложении группы G по нормальному делителю H.* Обозначение: $H \nabla G$.

ЗАМЕЧАНИЕ. Нетрудно проверить, что пересечение любого числа нормальных делителей группы $< G, \bullet >$ само является нормальным делителем этой группы.

ПРИМЕР **1**

В абелевой группе всякая подгруппа является нормальным делителем, поэтому, например, подгруппа всех четных чисел будет нормальным делителем аддитивной группы всех целых чисел $< Z, + >$.

ОПРЕДЕЛЕНИЕ. Элементы x и y группы G называются *сопряженными в G,* если:

$$(\exists\, g \in G)\ \ y = g^{-1} \bullet x \bullet g.$$

ТЕОРЕМА (*Критерий нормального делителя)*

Подгруппа H группы G тогда и только тогда будет нормальным делителем в $< G, \bullet >$, когда H вместе со всяким своим элементом будет содержать и все элементы, сопряженные с ним в G.

ТЕОРЕМА. Пусть H – нормальная подгруппа группы $< G, \bullet >$. Множество всех различных смежных классов группы G по подгруппе H с операцией умножения:

$$(H \bullet g_1) \bullet (H \bullet g_2) = H \bullet (g_1 \bullet g_2)$$

образует группу, которая называется *фактор-группой группы G по подгруппе H* и обозначается:

$$G / H = \{H \bullet g / \ g \in G\}.$$

Гомоморфизмы и изоморфизмы групп

ОПРЕДЕЛЕНИЕ. Отображение группы < *G,* • > на группу <S, * > называется *гомоморфизмом групп,* если выполняется условие:

$$(\forall\ a, b \in G)\ \ f(a \bullet b) = f(a) * f(b). \quad (1)$$

Сами группы называются при этом *гомоморфными.* Также говорят, что группа <S, * > есть *гомоморфный образ* группы < G, • >.

Обозначение: G ~ S.

ЗАМЕЧАНИЕ. Условие (1) из определения 1 называют также *требованием сохранения групповой операции.* Словами оно читается так: образ произведения элементов группы < G, • > равен произведению их образов в группе <S, * >.

Поэтому в правой части равенства (1) стоит знак операции « • » группы G, а в левой – знак операции « * » группы S.

ОПРЕДЕЛЕНИЕ. Гомоморфизм f групп G и S называется *изоморфизмом*, если отображение f биективно.

Сами группы называются при этом *изоморфными,* а группа <*S, * >* - *изоморфным образом* группы < G, • >. Обозначение: $G \cong S$.

Отметим некоторые свойства изоморфизмов групп.

СВОЙСТВО **1.** При изоморфизме групп нейтральный элемент переходит в нейтральный.

СВОЙСТВО **2.** При изоморфизме групп обратный элемент переходит в обратный:

$$(\forall\ a \in G)\ f(a^{-1}) = [f(a)]^{-1}.$$

СВОЙСТВО **3.** При изоморфизме групп сохраняется свойство коммутативности операции.

СВОЙСТВО **4.** Изоморфный образ группы является группой.

ПРИМЕР **1.** Аддитивная группа всех целых чисел изоморфна своей подгруппе, состоящей из четных чисел, так как отображение $\varphi: Z \to 2Z$ такое, что:

$$(\forall\ x \in Z)\ \ \varphi(x) = 2x,$$

является изоморфизмом групп, так как очевидно, что φ - биективно и $(\forall\ x, y \in Z)$ $\varphi(x + y) = 2(x + y) = 2x + 2y = \varphi(x) + \varphi(y)$.

ПРИМЕР **2.** Аддитивная группа всех действительных чисел изоморфна мультипликативной группе всех положительных действительных чисел:

$$<R, + > \ \cong\ <R^{+}, \bullet >,$$

так как отображение $\varphi: R \to R^{+}$, при котором:

$$(\forall\ x \in R)\ \ \varphi(x) = e^{x}$$

является биекцией, поскольку:

$$(\forall\ x, y \in R)\ \ \varphi(x) = \varphi(y) <=> e^{x} = e^{y} <=> x = y,$$

$$(\forall\ r \in R^{+})\ (\exists\ x \in R)\text{: } \varphi(x) = y, \text{ а именно, } x = \ln y, \text{ т.к. } \varphi(\ln y) = e^{\ln y} = y$$

и сохраняет групповую операцию:

$$(\forall\ x, y \in R)\ \varphi(x + y) = e^{x+y} = e^{x} \bullet e^{y} = \varphi(x) \bullet \varphi(y).$$

ТЕОРЕМА *(о гомоморфизме групп).* Если $\varphi: K \to S$ есть гомоморфизм группы G на группу S, то фактор-группа G / Ker φ изоморфна группе S.

При этом изоморфизм $\chi: S \to G$ / Ker φ можно выбрать таким образом, что для всех $x \in G$,будет выполняться равенство $\chi(\ \varphi(x)\ ) = \pi(x)$, где π - естественный гомоморфизм G на G / Ker φ .

5. Кольца и поля

ОПРЕДЕЛЕНИЕ. 1. Непустое множество A с заданными на нем бинарными операциями « ◦ » и « * » называется *полукольцом* < A, *, ◦ >, если:

1) < A, * > - абелева полугруппа, т.е., операция « * » ассоциативна, коммутативна и обладает нейтральным элементом;

2) < A, ◦ > - группоид;

3) операция « ◦ » связана с операцией « * » левым и правым законами дистрибутивности, т.е.

$$(\forall a, b, c \in A)\ c \circ (a * b) = (c \circ a) * (c \circ b)$$
$$\text{и} \quad (a * b) \circ c = (a \circ c) * (b \circ c).$$

2. Полукольцо $< A, *, \circ >$ называется *кольцом*, если:

1) $< A, * >$ - абелева группа, т.е. операция *« * »* ассоциативна, коммутативна, обладает нейтральным элементом и обратима;

2) $< A, \circ >$ - группоид;

3) операция *« ◦ »* связана с операцией *« * »* левым и правым законами дистрибутивности, т.е.,

$$(\forall a, b, c \in A)\ c \circ (a * b) = (c \circ a) * (c \circ b)$$
$$(a * b) \circ c = (a \circ c) * (b \circ c).$$

3. Кольцо $< A, *, \circ >$ называется *полем*, если:

1) $< A, * >$ - абелева группа, т.е. операция « * » ассоциативна, коммутативна, обладает нейтральным элементом и обратима;

2) $< A /\{0\}, \circ >$ -- абелева группа, т.е. операция « ◦ » ассоциативна, коммутативна, обладает нейтральным элементом и обратима;

3) операция « ◦ » связана с операцией « * » левым и правым законами дистрибутивности, т.е.

$$(\forall a, b, c \in A)\ c \circ (a * b) = (c \circ a) * (c \circ b)$$
$$(a * b) \circ c = (a \circ c) * (b \circ c).$$

ЗАМЕЧАНИЯ

1. Вообще, если на некотором непустом множестве A заданы две бинарные алгебраические операции « * » и « ◦ », то говорят, что задана *алгебраическая структура* $< A, *, \circ >$ *с двумя бинарными операциями.*

2. Так как по определению операция « * » коммутативна *в любом кольце*, то *коммутативным кольцом* называется такое кольцо, в котором коммутативна вторая операция *« ◦ ».* Обычно операцию « ◦ » называют *умножением,* а операцию « * » - *сложением* независимо от их природы. Аналогично, если речь идет об *ассоциативном кольце,* то этим свойством обладает операция умножения « ◦ ». Если по операции умножения в кольце существует нейтральный элемент, то кольцо называют *кольцом с единицей.*

ОПРЕДЕЛЕНИЕ. 1. Пусть на множестве A с элементом 0 задана операция «◦».

Элемент $x \in A$ называется *левым [правым] делителем нуля*, если:

1) $x \neq 0$;

2) $(\exists a \in A)\ a \neq 0$ и $x \circ a = 0$ [$a \circ x = 0$].

Если элемент $x \in A$ является и левым и правым делителем нуля, то его называют *двусторонним* (или просто) *делителем нуля.*

2. Ассоциативно-коммутативное кольцо без делителей нуля называется *областью целостности.*

ПРИМЕР **2.** 1. Множество N натуральных чисел по операции обычного умножения образует абелев моноид $< N, \bullet >$.

Множество N по операции обычного сложения также образует абелев моноид $< N, + >$, так как:

$$(\forall a, b \in N) \quad a + b \in N;$$
$$(\forall a, b, c \in N)\ a + (b + c) = (a + b) + c;$$
$$(\forall a, b \in N) \quad a + b = b + a;$$
$$(\forall a \in N) \quad a + 0 = 0 + a = a;$$

однако операция сложения не обратима на N, так как, например, для числа 2 не существует обратного (противоположного) элемента в множестве N.

Так как $(\forall a, b, c \in N)\ c \cdot (a + b) = c \cdot a + c \cdot b$, то умножение на N дистрибутивно относительно сложения.

Из сказанного следует, что структура $< N, +, \bullet >$ образует ассоциативно-коммутативное полукольцо с единицей.

2. Очевидно также, что умножение на множестве Z всех целых чисел обладает такими же свойствами, как и сложение, кроме свойства обратимости, поскольку для всякого целого числа a, за исключением 1 и -1, обратный элемент a^{-1} не является целым числом. Поэтому структура < Z, ·> образует абелеву полугруппу. Кроме того, очевидно, что в множестве Z нет делителей нуля. Следовательно, структура < Z, +, ·> является областью целостности.

3. Нетрудно проверить, что на множестве всех действительных чисел сложение и умножение обладают свойствами ассоциативности, коммутативности, в качестве нейтральных элементов выступают 0 и 1 соответственно, обе операции обратимы и умножение дистрибутивно относительно сложения. Следовательно, < R, +, ·> по операциям сложения и умножения образует поле.

Рассмотрим еще один пример, который будет иметь особое значение в дальнейшем.

ПРИМЕР **3.** На множестве Z_m определим операции сложения и умножения вычетов по правилам:

$$\overline{a} + \overline{b} = \overline{a + b},$$
$$\overline{a} \cdot \overline{b} = \overline{a \cdot b}.$$

Нетрудно проверить, что эти операции на множестве Z_m всегда выполнимы и однозначно определены, то есть результат выполнения операции не зависит от выбора представителя класса вычетов. В получающейся таким образом алгебре < Z_m, +, • > выполняются все аксиомы коммутативного кольца с единицей. Кольцо <Z_m, +, • > называется *кольцом классов вычетов* или просто *кольцом вычетов по модулю m*.

Справедливы следующие утверждения, которые будут нам полезны в дальнейшем.

ТЕОРЕМА. Элемент a кольца Z_m имеет обратный тогда и только тогда, когда

НОД(a, m) = 1.

ТЕОРЕМА

Кольцо вычетов < Z_m, +, ·> тогда и только тогда является полем, когда m – простое число.

Простейшие свойства колец и полей. Гомоморфизмы и изоморфизмы колец и полей

СВОЙСТВО **1.** Всякая аддитивная абелева группа <G, + > может служить аддитивной группой кольца <G, + , • >, где умножение *« • »* определено следующим образом:

$$(\forall\ a, b \in G)\ a \bullet b = 0.$$

СВОЙСТВО **2.** В любом кольце выполняются все свойства аддитивной группы.

СВОЙСТВО **3.** Во всяком кольце <K, + , • > умножение дистрибутивно слева и справа относительно вычитания:

$$(\forall\ a, b, c \in K)\ c \bullet (a - b) = c \bullet a - c \bullet b \text{ и}$$
$$(a - b) \bullet c = a \bullet c - b \bullet c.$$

СВОЙСТВО **4**

Во всяком кольце <K, + , • > любое произведение, в котором хотя бы один из сомножителей равен нулю, само равно нулю, то есть:

$$(\forall\ a \in K)\ a \bullet 0 = 0 \bullet a = 0.$$

ЗАМЕЧАНИЕ. Обращение последнего свойства, вообще говоря, неверно. А именно, существуют кольца, например, кольцо квадратных матриц порядка *n*, в которых из равенства нулю произведения a • b = 0 не следует равенство нулю сомножителей. То есть, существуют кольца с *делителями нуля.*

ОПРЕДЕЛЕНИЕ. *Подкольцом* кольца К называется всякое подмножество К′ этого кольца, которое само является кольцом относительно операций, определенных в К.

ТЕОРЕМА *(критерий подкольца)*

Подмножество K′ кольца <K, + , • > будет его подкольцом тогда и только тогда, когда выполнены условия:

1) (∀ a, b ∈ K′) a + (-b) ∈ K′ , т.е., < K′ , + > - подгруппа аддитивной группы кольца*;*

2) (∀ a, b ∈ K′) a • b ∈ K′ .

СВОЙСТВО **5.** Так как всякое поле является кольцом, то все свойства колец справедливы и для полей.

ОПРЕДЕЛЕНИЕ. Пусть дано кольцо <K, + , • >. Рассмотрим множество P всех таких упорядоченных пар элементов кольца K, у которых второй элемент не равен нулю:

$$P = \{<a, b>/\ a, b \in K, b \neq 0\}.$$

Будем обозначать такие пары в виде дробей $\frac{a}{b}$ и называть их частными кольца <K, + , • >. Зададим на множестве всех частных кольца операции « + » и «•» следующим образом:

$$(\forall\ a, b, c, d \in K) \quad \frac{a}{b} + \frac{c}{d} = \frac{a \bullet d + c \bullet b}{b \bullet d},\ b \neq 0,\ d \neq 0;$$

$$(\forall\ a, b, c, d \in K) \quad \frac{a}{b} \bullet \frac{c}{d} = \frac{a \bullet c}{b \bullet d},\ b \neq 0,\ d \neq 0.$$

ОПРЕДЕЛЕНИЕ. Два частных будем называть равными, если выполняется равенство:

$$\frac{a}{b} = \frac{c}{d} \iff a \bullet d = b \bullet c.$$

Множество всех равных между собой частных поля K будем объединять в один класс и в качестве представителя этого класса обычно рассматривается несократимая дробь, которая в данном классе единственна.

Нетрудно проверить, что операции заданы корректно, то есть результат их выполнения не зависит от выбора представителя класса. Поэтому в дальнейшем будем отождествлять весь класс равных между собой частных кольца с его несократимым представителем.

Следующие свойства множества всех частных кольца K показывают, что по заданным операциям это множество образует поле, которое называется *полем частных кольца K.*

СВОЙСТВО **6.** Операции сложения и умножения на множестве всех частных кольца K обладают свойствами ассоциативности и коммутативности. Умножение связано со сложением левым и правым законами дистрибутивности.

СВОЙСТВО **7.** По операции « + » существует нейтральный элемент, в качестве которого выступает класс дробей с числителем, равным нулю, и произвольным знаменателем.

Для элемента $\frac{a}{b}$ противоположным является элемент $\frac{-a}{b}$.

СВОЙСТВО **8.** По операции « • » существует нейтральный элемент, в качестве которого выступает класс дробей с числителем, равным знаменателю. Для всякого ненулевого элемента $\frac{a}{b}$ обратным является элемент $\frac{b}{a}$.

СВОЙСТВО **9.** Единица поля не равна нулю поля, следовательно, во всяком поле имеется по крайней мере два различных элемента – 0 и 1.

СВОЙСТВО **10.** Никакое поле не содержит делителей нуля.

ОПРЕДЕЛЕНИЕ. Пусть <K, + , •> и <S, ∗ , °> - два кольца. Отображение φ: K → S называется *гомоморфизмом колец,* если выполняются условия:

1) $(\forall\ a, b \in K)\ \varphi(a + b) = \varphi(a) * \varphi(b)$;

2) $(\forall\ a, b \in K)\ \varphi(a \bullet b) = \varphi(a) \circ \varphi(b)$.

Гомоморфизм φ колец K и S называется *изоморфизмом,* если отображение φ биективно.

ОПРЕДЕЛЕНИЕ. *Ядром гомоморфизма* колец K и S называется множество всех элементов кольца K, которые отображаются в нуль кольца S:

$$\mathrm{Ker}\ \varphi = \{x \mid x \in K, \varphi(x) = 0_S\}.$$

Тема. Теория делимости в кольце целых чисел и кольце многочленов

План

1. Деление целых чисел с остатком.

2. НОД и НОК целых чисел. Алгоритм Евклида. Каноническое представление целых чисел.

3. Деление многочленов с остатком. Деление многочлена на двучлен. Корни многочлена

4. НОД и НОК многочленов. Алгоритм Евклида и теорема Ламе для многочленов.

1. Деление целых чисел с остатком

ОПРЕДЕЛЕНИЕ. Говорят, что целое число a *делится* на целое число $b \neq 0$, если найдется такое целое число c, что $a = b \cdot c$.

Число a называется *кратным числа b,* число b – *делителем числа a,* число c – *частным от деления a на b.*

ЗАМЕЧАНИЕ. Отношение делимости, как видно из определения, вводится через обратную операцию – умножение целых чисел. Однако, если рассматривать деление как бинарную операцию, которая паре целых чисел $\langle a, b\rangle$, $b \neq 0$, ставит в соответствие число $a : b$, которое, вообще говоря, не обязательно является целым, то операция деления на множестве Z будет *частичной операцией.*

Отметим основные свойства отношения делимости в кольце Z.

СВОЙСТВО **1.** Пусть a и b – целые числа, не равные 0. Если одновременно выполняются условия: $a : b$ и $b : a$, то $a = \pm b$.

Если $a : b$, то $a : -b$ и $-a : b$. Целое число 0 делится на любое другое целое число.

СВОЙСТВО **2.** Если для целых чисел a, b и $c \neq 0$ выполняются условия:

$$a : b \text{ и } a : c, \text{ то } a : (b \pm c).$$

ЗАМЕЧАНИЕ. Обратное утверждение в общем случае неверно, то есть, если для целых чисел a, b и c выполняется делимость $a : (b \pm c)$, то отсюда не следует, что число a делится на каждое из слагаемых. Например, $12 : (5 + 7)$, но при этом 12 не делится ни на 5, ни на 7.

СВОЙСТВО **3.** Отношение делимости на множестве $Z \setminus \{0\}$ рефлексивно и транзитивно, так как:

$$(\forall\ a \in Z \setminus \{0\})\ a : \pm a \quad \text{и}$$

$$(\forall\ a, b, c \in Z \setminus \{0\})\ (a : b \text{ и } b : c \Rightarrow b : c).$$

Очевидно, что на множестве Z^+ отношение делимости будет также антисимметрично, так как:

$$(\forall\ a, b \in Z^+)\ (a : b \text{ и } b : a \Rightarrow a = b).$$

Поэтому на множестве всех положительных целых чисел отношение делимости является отношением нестрогого порядка.

СВОЙСТВО **4.** Если для целых a и $b \neq 0$, $a : b$, то для любого целого c: $ac : b$.

СВОЙСТВО **5.** Если каждое из двух целых чисел a и b делится на число $c \neq 0$, то: $(\forall\ n, m \in Z)\ (na \pm mb) : c$.

ОПРЕДЕЛЕНИЕ. Говорят, что целое число *a делится с остатком* на целое число $b \neq 0$, если существуют такие целые числа p и q, что выполняются условия:

$$a = bq + r,\ 0 \le r < |b|\ (*).$$

Число q называется *неполным частным*, а число r – *остатком* от деления a на b.

Из определения, вообще говоря, нельзя сделать выводов о том, всегда ли существует такая пара целых чисел q и r и однозначно ли они определены для данных a и b. Ответ на эти вопросы дает соответствующая теорема.

ТЕОРЕМА *(о делении целых чисел с остатком).* Для всяких целых чисел a и b, где $b \neq 0$, деление с остатком всегда выполнимо и однозначно определено.

Иными словами, для всяких целых чисел a и b, где $b \neq 0$, всегда существует и притом единственная пара целых чисел q и r, удовлетворяющих условию (*).

ЗАМЕЧАНИЕ. Если заданы числа a и q или a и r, то другую пару чисел из условия (*) можно подобрать не одним способом.

СВОЙСТВО **1.** Числа a и b дают одинаковые остатки при делении на некоторое целое число m тогда и только тогда, когда разность (a – b) делится на m нацело.

Пусть m – некоторое целое число, $m \neq 0$, $m \neq 1$. Рассмотрим на множестве Z бинарное отношение ρ :

$(\forall\ a, b \in Z)$ <a, b> $\in \rho$ <=> числа a и b при делении на m дают одинаковые остатки.

Тогда справедливо следующее свойство.

СВОЙСТВО **2.** Отношение ρ на множестве целых чисел является отношением эквивалентности. Оно разбивает все множество Z на классы эквивалентности, в каждый из которых попадают те и только те целые числа, которые при делении на m дают один и тот же остаток r. Так как различными остатками при делении на m могут быть числа 0, 1, 2, … m – 1, то существует ровно m различных классов разбиения по данному отношению ρ:

$$K_r = \{a \in Z / a = xq + r, x, q \in Z\}.$$

Любое целое число, принадлежащее классу K_r, называют его *представителем.*

Обозначим множество вех классов разбиения по отношению эквивалентности ρ через Z / ρ :

$$Z / \rho = \{K_0, K_1, \ldots, K_{\hat{e}}, \ldots, K_{m-1}\}$$

и зададим на этом множестве операции сложения и умножения классов:

$$K_r + K_s = K_{r+s};$$

$$K_r \cdot K_s = K_{rs}, \text{ где } r, s \in \{0, 1, \ldots, m\text{-}1\}.$$

Нетрудно проверить, что операции определены корректно и результат их выполнения не зависит от выбора представителя класса. Тогда можно сформулировать следующие свойства.

СВОЙСТВО **3.** Операция сложения на множестве Z / ρ ассоциативна и коммутативна. Нейтральным элементом является класс K_0, противоположным элементом для класса K_r является класс K_s, где s – наименьшее целое положительное число со свойством: сумма (r + s) делится на m нацело.

СВОЙСТВО **4.** Операция умножения на множестве Z/ρ ассоциативна, коммутативна и обладает единицей, которой является класс K_1.

СВОЙСТВО **5.** Умножение классов связано со сложением законами дистрибутивности:

$$K_r \cdot (K_s + K_t) = K_r \cdot K_{s+t} = K_{r(s+t)} = K_{rs+rt} = K_{rs} + K_{rt} = K_r \cdot K_s + K_r \cdot K_t.$$

СВОЙСТВО **6**

Из свойств 4 – 6 следует, что множество Z / ρ по операциям сложения и умножения классов образует кольцо, которое называется *кольцом классов вычетов по модулю m*.

ЗАМЕЧАНИЕ. Можно показать, что фактор-кольцо кольца Z из примера 2

параграфа 2.6 вида Z / mZ будет изоморфно кольцу классов вычетов по модулю m. Поэтому кольца вида Z / mZ также называют кольцами классов вычетов по модулю m.

2. НОД и НОК целых чисел. Алгоритм Евклида. Каноническое представление целых чисел

НОД и НОК целых чисел

ОПРЕДЕЛЕНИЕ. Целое число $d \neq 0$ называется *общим делителем* целых чисел a и b, если каждое из этих чисел делится на число d.

Общий делитель чисел a и b называется их *наибольшим общим делителем*, если он делится на любой другой их общий делитель.

Обозначение: $d = НОД(a, b)$ или $d = (a, b)$.

Отметим некоторые свойства НОД целых чисел, которые будут важны в дальнейшем.

СВОЙСТВО **1.** Если $d = НОД(a, b)$ и $d_1 = НОД(a, b)$, то $d_1 = \pm d$.

СВОЙСТВО **2.** Если число a делится на число $b \neq 0$ нацело, то $НОД(a, b) = b$.

СВОЙСТВО **3.** Пусть $d_1 = НОД(a, b)$, $d = НОД(d_1, c)$, тогда $d = НОД(a, b, c)$.

СВОЙСТВО **4.** Если число a делится на число b с остатком, то есть

$$a = bq + r,\ 0 \leq r < |b|, \text{ то } НОД(a, b) = НОД(b, r).$$

ЗАМЕЧАНИЯ

1. Первое свойство означает, что НОД двух целых чисел определен с точностью до знака. Обычно принято проводить рассуждения с положительным значением НОД целых чисел.

2. Третье свойство фактически утверждает, что операция нахождения НОД целых чисел ассоциативна, так как:

$$НОД(НОД(a, b), c) = НОД(a, (НОД(b, c)) = НОД(a, b, c).$$

Это означает, что вычислять НОД нескольких целых чисел можно в произвольном порядке.

ОПРЕДЕЛЕНИЕ. Целое число h называется *общим кратным* ненулевых целых чисел a и b, если h делится на каждое из этих чисел.

Общее кратное целых чисел a и b называется их *наименьшим общим кратным*, если на него делится любое другое их общее кратное. Обозначение: $h = НОК(a, b)$ или $h = [a, b]$.

Отметим некоторые свойства НОК целых чисел, которые схожи со свойствами наибольшего общего делителя.

СВОЙСТВО **1.** Если $h = НОК(a, b)$ и $h_1 = НОК(a, b)$, то $h_1 = \pm h$.

СВОЙСТВО **2.** Если число a делится на число $b \neq 0$ нацело, то $НОК(a, b) = a$.

СВОЙСТВО **3.** Пусть $h_1 = НОК(a, b)$ и $h = НОК(h_1, c)$, тогда $h = НОК(a, b, c)$.

ЗАМЕЧАНИЯ

1. Первое свойство означает, что НОК двух целых чисел определено с точностью до знака.

2. Третье свойство утверждает ассоциативность операции нахождения НОК целых чисел: НОК нескольких целых чисел можно вычислять в произвольном порядке.

$$НОК(НОК(a, b), c) = НОК(a, (НОК(b, c)) = НОК(a, b, c).$$

Алгоритм Евклида. Теорема Ламе

Заметим, что из определения и свойств наибольшего общего делителя и наименьшего общего кратного целых чисел не следует, что НОД и НОК двух чисел всегда существуют. Их существование нужно доказывать отдельно.

Пусть a, $b \neq 0$ – целые числа. Построим для них так называемую *последовательность Евклида,* выполняя последовательно деление с остатком.

1) Если a делится на b нацело, то последовательность Евклида имеет вид: *a, b*.

2) Пусть $a > b$ и a не делится на b нацело. Тогда, выполняя деление a на b с остатком, получим:

$$a = bq_0 + r_0,\ 0 \leq r_0 < |b|.$$

Затем делим число b на полученный остаток r_0:

$$b = r_0 q_1 + r_1,\ 0 \le r_1 < r_0.$$

Снова делим теперь уже r_0 на остаток r_1:

$$r_0 = r_1 q_2 + r_2,\ 0 \le r_2 < r_1.$$

Продолжаем процесс деления с остатком до тех пор, пока на некотором шаге не получим остаток, равный нулю:

$$r_{n-2} = r_{n-1} q_n + r_n,\ 0 \le r_n < r_{n-1},$$

$$r_{n-1} = r_n q_{n+1} + 0.$$

Последовательность, полученная в ходе этих операций:

$$a > b > r_0 > r_1 > \ldots > r_{n-1} > r_n > r_{n+1} = 0 \quad (**),$$

и будет последовательностью Евклида для случая 2).

Последовательность (**) обязательно оборвется на нуле через конечное число шагов, так как она является строго убывающей последовательностью натуральных чисел (начиная с r_0). Множество натуральных чисел ограничено снизу нулем, поэтому последовательность (**) не может убывать бесконечно.

Алгоритм построения последовательности Евклида называется *алгоритмом Евклида,* который используется при доказательстве существования НОД двух целых чисел.

ТЕОРЕМА *(о существовании НОД целых чисел).* Пусть a и b ≠ 0 – целые числа. Алгоритм Евклида доставляет НОД чисел a и b, который равен последнему не равному нулю остатку в последовательности Евклида (**):

$$НОД\ (a, b) = r_n.$$

ТЕОРЕМА *(о существовании НОК целых чисел).* Пусть a и b – не равные нулю целые числа. Тогда справедливо соотношение:

$$НОК\ (a, b) = \frac{ab}{НОД\ (a,b)} \quad (***).$$

ЗАМЕЧАНИЕ. В связи с использованием алгоритма Евклида возникает вопрос: сколько шагов необходимо выполнить для вычисления НОД? Ответ на этот вопрос дает теорема, доказанная французским математиком, физиком и инженером Габриэлем Ламе (1795-1870).

ТЕОРЕМА *(Ламе).* Пусть a и b - натуральные числа. Число шагов в алгоритме Евклида для чисел a и b не превосходит 5k, где k - число десятичных цифр меньшего из чисел a и b.

ТЕОРЕМА. Пусть d = НОД (a, b). Тогда существуют такие целые числа x и y, что d линейно выражается через сами числа a и b:

$$d = xa+yb,\ x, y \in Z. \quad (1)$$

Алгоритм, позволяющий вычислять числа x и y, удовлетворяющие равенству (1) для данных чисел a и b и их наибольшего общего делителя d, получил название *расширенного алгоритма Евклида,* который заключается в следующем.

Из каждого равенства, которые получаются при построении последовательности Евклида, выразим остаток и подставим его в следующее равенство, пока не дойдем до НОД чисел a и b. В последнем равенстве приведем подобные слагаемые при этих числах. Полученные коэффициенты и будут численными значениями x и y:

$$r_0 = a - bq_0,\ r_1 = b - r_0 q_1,\ \Rightarrow r_1 = b - (a - bq_0)\, q_1,$$ и т.д.

ОПРЕДЕЛЕНИЕ. Натуральное число p называется *простым*, если оно не имеет других делителей, кроме себя и единицы. Если же число имеет делители, отличные от себя и единицы, то оно называется *составным.*

ПРИМЕР 1. Числа 2, 3, 19, 31 являются простыми, а числа 6, 222, 18, 864 – составными.

ЗАМЕЧАНИЕ. Единица, очевидно, не является ни простым, ни составным

числом. Можно сказать, что множество всех натуральных чисел разбивается на три непересекающихся класса: класс простых чисел, класс составных чисел и класс, содержащий только единицу.

СВОЙСТВО **1.** Всякое составное число a имеет хотя бы один простой делитель p, не превосходящий $\sqrt{a}$: p ≤ $\sqrt{a}$.

СВОЙСТВО **2.** Если произведение двух целых чисел делится на простое число *p*, то хотя бы один из сомножителей делится на это число:

$$ab : p \Rightarrow a : p \text{ или } b : p.$$

СВОЙСТВО **3.** Если p и q – простые числа и p : q, то p = q.

Простые числа играют особую роль среди всех натуральных, и даже целых чисел, которая выражается следующей теоремой.

ТЕОРЕМА *(основная теорема арифметики).* Всякое натуральное число может быть представлено в виде произведения простых сомножителей единственным образом с точностью до порядка следования сомножителей.

ЗАМЕЧАНИЯ

1. Теорема справедлива и для целых чисел, так как всякое целое число a можно представить в виде:

$$a = \varepsilon_a |a| \text{ – где } \varepsilon_a \text{ - знак, } a|a| \text{ - натуральное число.}$$

2. Если в разложении целого числа *a* на простые множители собрать вместе в виде степени одинаковые простые числа, то полученное разложение называется *канонической формой записи числа* a*:*

$$a = \varepsilon_a \, p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdot \ldots \cdot p_k^{\alpha_k}, \qquad (2)$$

где $p_1, p_2, \ldots, p_k$ - различные простые множители.

Основная теорема арифметики также может использоваться для нахождения НОД и НОК целых чисел по следующим правилам, которые следуют из определения и свойств делимости и свойств простых чисел.

ПРАВИЛО **1.** Чтобы найти НОД двух (или нескольких) целых чисел, нужно в их каноническом разложении на простые множители выбрать все множители, которые входят в разложения каждого из чисел, причем в наименьшей степени, и перемножить их.

ПРАВИЛО **2.** Чтобы найти НОК двух (или нескольких) целых чисел, нужно в их каноническом разложении на простые множители выбрать все множители, которые входят в разложение хотя бы одного из чисел, причем в наибольшей степени, и перемножить их.

Основной факт, который был установлен о множестве простых чисел, выражается следующей теоремой.

ТЕОРЕМА. Множество простых чисел бесконечно.

ОПРЕДЕЛЕНИЕ. Два целых числа a и b называются *взаимно-простыми*, если они не имеют других общих делителей кроме единицы.

СВОЙСТВО **4.** Числа a и b взаимно-просты тогда и только тогда, когда их НОД равен единице: НОД *(a, b) = 1.*

СВОЙСТВО **5.** Если числа a и b взаимно-просты, то существуют такие целые числа x и y, что: ax + by = 1.

СВОЙСТВО **6.** Если числа a и b взаимно-просты, то НОК(a, b) = ab.

КИТАЙСКАЯ ТЕОРЕМА ОБ ОСТАТКАХ. Пусть $m_1, m_2, \ldots, m_k$ — попарно взаимно простые числа, α — целое число. Для любого набора $j_1, j_2, \ldots, j_k$, $(0 \le j_i < m_i)$ существует единственное целое число γ, удовлетворяющее условиям*:*

$$\gamma \equiv j_i (\mathrm{mod}\ m_i), \text{ где } i = 1,2,\ldots,k \text{ и } \alpha \le \gamma < \alpha + m_1 m_2 \cdots m_k..$$

3. Деление многочленов с остатком. Деление многочлена на двучлен. Корни многочлена

ОПРЕДЕЛЕНИЕ. Пусть P – некоторое поле. *Многочленом от одной переменной над полем P* будем называть формальную сумму вида:

f(x) = $a_n x^n + a_{n-1}x^{n-1} + ... + a_1 x + a_0$, где $a_i \in P$, $i \in \{0, 1, \ldots, n\}$, $n \in N$. (1)

Числа a_i называют *коэффициентами* многочлена f(x). Если $a_n \neq 0$, то число n называют *степенью многочлена f(x)*, a_n - *старшим коэффициентом,* a_0 - *свободным членом многочлена f(x).* Одночлен $a_n x^n$ называется в этом случае *старшим членом.*

Если старший коэффициент многочлена равен единице, то многочлен называется *нормированным*.

ЗАМЕЧАНИЯ

1. Всякий элемент поля P будем считать многочленом нулевой степени, многочлен произвольной степени с нулевыми коэффициентами – нулевым многочленом, единицу поля P – единичным многочленом и обозначать их $\vartheta(x)$ и E(x) соответственно.

Не следует путать многочлен *нулевой степени* с *нулевым* многочленом!

2. Вместо записи (1) иногда будем использовать запись: f(x) = $\sum_{i=0}^{n} a_i x^i$ (2)

На множестве всех многочленов от одной переменной над полем P можно задать операции сложения и умножения многочленов по следующим правилам. Пусть f(x) – многочлен вида (1) и g(x) = $b_m x^m + b_{m-1}x^{m-1} + ... + b_1 x + b_0$, где $b_j \in P$, $j \in \{0, 1, \ldots, m\}$, $m \in N$ – многочлен вида (2).

ОПРЕДЕЛЕНИЕ. *Суммой* многочленов f(x) и g(x) назовем многочлен h(x) вида: h(x) = $c_k x^k + c_{k-1}x^{k-1} + ... + c_1 x + c_0$, где $c_i = a_i + b_i$, $i \in \{0, 1, \ldots, k\}$, $k = \max\{n, m\}$. (3)

ЗАМЕЧАНИЕ. Для удобства в многочлене меньшей степени будем представлять недостающие степени в виде одночленов с нулевыми коэффициентами, т.е., если f(x) = $\sum_{i=1}^{6} a_i x^i$, g(x) = $\sum_{j=1}^{4} b_j x^j$, то представим g(x) в виде: g(x) = $0x^6 + 0x^5 + b_4 x^4 + b_3 x^3 + b_2 x^2 + b_1 x + b_0$.

ОПРЕДЕЛЕНИЕ. *Произведением* многочленов f(x) и g(x) будем называть многочлен h(x) вида: h(x) = $(\sum_{i=0}^{n} a_i x^i) \bullet (\sum_{j=0}^{m} b_j x^j) = \sum_{k=0}^{n+m} c_k x^k$, где $c_k = a_0 b_k + a_1 b_{k-1} + a_2 b_{k-2} + ... + a_k b_0$.

Иными словами, чтобы найти произведение двух многочленов, нужно каждый одночлен первого сомножителя умножить на каждый одночлен второго и затем привести подобные слагаемые.

ЗАМЕЧАНИЕ. Так как мы рассматриваем многочлены над полем, а в поле нет делителей нуля, то старший член произведения двух многочленов всегда будет равен произведению их старших членов. В общем же случае это не так. Если коэффициенты взяты из произвольного кольца, то может оказаться, что произведение двух старших ненулевых коэффициентов, тем не менее, равно нулю.

Нетрудно проверить, что сложение и умножение многочленов над полем обладают свойствами коммутативности и ассоциативности, умножение дистрибутивно относительно сложения, нейтральным элементом по сложению является нулевой многочлен $\vartheta(x)$, а элементом, противоположным многочлену f(x), – многочлен, коэффициенты которого есть числа, противоположные (в поле P) коэффициентам данного многочлена. Поэтому справедлива теорема.

ТЕОРЕМА. Множество всех многочленов от одной переменой над полем P по заданным операциям сложения и умножения многочленов образует кольцо, которое называется *кольцом многочленов от одной переменной* и обозначается P[x].

ЗАМЕЧАНИЕ. Из предыдущего замечания следует, что кольцо P[x] над полем P является областью целостности.

ОПРЕДЕЛЕНИЕ. Число x_0 называется *корнем многочлена* f(x), если: $f(x_0) = \sum_{i=0}^{n} a_i x_0^i = 0$.

ЗАМЕЧАНИЕ. Если подставить в выражение (1) вместо переменой x некоторое число α из поля P и произвести необходимые действия, то полученное в результате число называется значением многочлена f(x) при x = α.

Учитывая это, корень многочлена можно определить как число, на котором многочлен принимает значение, равное нулю.

В кольце многочленов P[x] над полем P можно задать частичную операцию – деление многочленов, подобно тому, как это было сделано в кольце целых чисел.

ОПРЕДЕЛЕНИЕ. Говорят, что многочлен f(x) вида (1) *делится* на многочлен g(x) вида (2), если найдется такой многочлен h(x) над полем P, что f(x) = g(x)·h(x).

Нулевые коэффициенты в записи многочленов появились для удобства вычисления.

Отметим некоторые простейшие свойства делимости многочленов, аналогичные свойствам делимости целых чисел.

СВОЙСТВО **1.** Если одновременно выполняется делимость многочлена f(x) на g(x) и обратно, то многочлены отличаются только на множитель нулевой степени или, иными словами, просто на числовой множитель c: f(x) = c g(x).

Многочлены f(x) и g(x) называются в этом случае *ассоциированными.*

Очевидно, что среди многочленов, ассоциированных с данным ненулевым многочленом, имеется ровно один нормированный многочлен.

СВОЙСТВО **2.** Если многочлен f(x) делится на каждый из двух многочленов g(x) и h(x), то он делится и на их произведение.

СВОЙСТВО **3.** Отношение делимости многочленов в кольце P[x] рефлексивно и транзитивно.

СВОЙСТВО **4.** Если многочлен f(x) делится на ненулевой многочлен g(x), то и любой многочлен, ассоциированный с f(x), будет делиться на g(x).

СВОЙСТВО **5.** Если каждый из двух многочленов f(x) и g(x) делится на ненулевой многочлен h(x), то и любая их линейная комбинация делится на h(x).

ОПРЕДЕЛЕНИЕ. Говорят, что многочлен f(x) *делится с остатком* на ненулевой многочлен g(x), если найдется такая пара многочленов q(x) и r(x), для которых выполняется равенство:

f(x) = g(x)·q(x) + r(x), причем степень r(x) $<$ степени g(x) или r(x) = ϑ(x) (1)

В кольце многочленов, также как и в кольце целых чисел, можно доказать теорему о делении с остатком.

ТЕОРЕМА *(о делении с остатком).* Для всякой пары многочленов f(x) и g(x), где g(x) - ненулевой многочлен, существует и притом единственная пара многочленов q(x) и r(x), которые удовлетворяют условиям (1).

Рассмотрим более подробно частный случая деления многочленов: деление многочлена на двучлен, так как он дает некоторые интересные и полезные на практике результаты.

ТЕОРЕМА. Остаток от деления многочлена f(x) на двучлен x – c равен значению многочлена f(x) при x = c: f(x) = (x – c)·q(x) + f(c).

Пусть многочлен f(x) записан в следующем виде:

$$f(x) = a_0 x^n + a_1 x^{n-1} + \ldots + a_{n-1} x + a_{n,} (a_0 \neq 0) \quad (1).$$

Представим его в виде:

$$f(x) = (x - c)\cdot(b_0 x^{n-1} + b_1 x^{n-2} + \ldots + b_{n-2} x + b_{n-1}) + r \quad (2)$$

Раскрывая мысленно скобки в правой части равенства и приравнивая коэффициенты при одинаковых степенях в равенствах (1) и (2), получим:

$$\begin{aligned} b_0 &= a_0, \\ b_1 &= a_1 + cb_0, \\ b_2 &= a_2 + cb_1, \\ &\cdots\cdots\cdots\cdots \\ b_k &= a_k + cb_{k-1}, \\ &\cdots\cdots\cdots\cdots \\ b_{n-1} &= a_{n-1} + cb_{n-2}, \\ r &= a_n + cb_{n-1}. \end{aligned} \qquad (3)$$

Вычисления (3) обычно записывают в виде таблицы и называют *схемой Горнера:*

	a_0	a_1	…	a_k	…	a_n
$x = c$	b_0	$b_1 = a_1 + cb_0$	…	$b_k = a_k + cb_{k-1}$	…	$r = a_n + cb_{n-1}$

Очевидно, что r = f(c), коэффициенты b_i есть коэффициенты частного *q(x)* от деления f(x) на x – c.

Схему Горнера удобно использовать также для разложения многочлена f(x) по степеням разности x – c.

ТЕОРЕМА. Для любого числа *c* из поля P многочлен f(x) вида (1) степени n всегда можно представить и притом единственным образом в виде:

$$\text{f(x)} = b_0 + b_1 \cdot (x-c) + b_2 \cdot (x-c)^2 + \ldots + b_n \cdot (x-c)^n, (b_n \neq 0). \quad (4)$$

Представление в виде (4) и называется *разложением f(x) по степеням разности x – c*.

Используя формулу Тейлора и схему Горнера, можно также находить значения производных различных порядков для многочлена f(x) в точке x = c.

ТЕОРЕМА. В разложении (4) многочлена f(x) по степеням разности x – c, коэффициенты b_k определяются следующим образом:

$$b_k = \frac{f^{(k)}(c)}{k!}, (k \in \{0, 1, 2, \ldots, n\}) \quad (5).$$

Корни многочлена

Учитывая понятие кратности корня, можно сформулировать следующие утверждения о числе корней многочлена f(x).

ЛЕММА

Всякий ненулевой многочлен может быть представлен в виде:

$$\text{f(x)} = (x-x_1)^{k_1} \cdot (x-x_2)^{k_2} \cdot \ldots \cdot (x-x_m)^{k_m} \cdot g(x) \quad (1).$$

где $x_1, x_2, \ldots, x_m$ - различные числа, а $g(x)$ - многочлен, не имеющий корней.

ЛЕММА. Если многочлен f(x) представлен в виде (1), то $x_1, x_2, \ldots, x_m$ - это все его корни, причем кратность корня x_i равна k_i.

ТЕОРЕМА. Сумма кратностей всех корней ненулевого многочлена f(x) не превосходит его степени, причем равенство имеет место тогда и только тогда, когда многочлен можно представить в виде произведения множителей первой степени.

Существуют равенства, выражающие связь корней многочлена с его коэффициентами. Пусть многочлен f(x) = $a_0 x^n + a_1 x^{n-1} + \ldots + a_{n-1} x + a_{n,} (a_0 \neq 0)$ имеет корни $x_1, x_2, \ldots, x_n$, причем они не обязательно различны. Тогда справедливы равенства:

$$
\begin{aligned}
a_1 &= -a_0 \cdot (x_1 + x_2 + ... + x_n), \\
a_2 &= a_0 \cdot (x_1x_2 + x_1x_3 + ... + x_{n-1}x_n), \\
&\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \\
a_n &= (-1)^n \cdot a_0 \cdot x_1x_2...x_n.
\end{aligned}
\qquad (6)
$$

Равенства (6) называются *формулами Виета,* выражающими коэффициенты многочлена f(x) через его корни и старший коэффициент.

4. НОД и НОК многочленов. Алгоритм Евклида и теорема Ламе для многочленов

Определение и простейшие свойства наибольшего общего делителя и наименьшего общего кратного многочленов аналогичны простейшим свойствам наибольшего общего делителя и наименьшего общего кратного целых чисел (сформулировать самостоятельно).

Остановимся на некоторых особенностях, присущих НОД и НОК многочленов.

ЗАМЕЧАНИЕ. НОД целых чисел, как известно, определен однозначно с точностью до знака. НОД многочленов определен однозначно с точностью до множителя нулевой степени, поскольку очевидно, что если d(x) = НОД (f(x), g(x)), то и любой ассоциированный с d(x) многочлен также будет являться НОД (f(x), g(x)).

Поскольку в кольце многочленов над полем выполнимо деление с остатком, то доказать существование НОД многочленов также можно с помощью алгоритма Евклида.

ТЕОРЕМА. Для всяких двух многочленов f(x) и g(x) существует их НОД, который равен последнему ненулевому остатку в последовательности Евклида.

ЗАМЕЧАНИЕ. Из предыдущего замечания следует, что для удобства вычислений при нахождении НОД двух многочленов можно домножать остатки, делимые или делители, которые получаются в процессе последовательных делений на любое ненулевое число.

ЗАМЕЧАНИЕ. В кольце многочленов над полем также выполняется расширенный алгоритм Евклида, который позволяет вычислить такие многочлены *u(x)* и *v(x)*, которые удовлетворяют равенству: НОД (f(x), g(x)) = u(x)·f(x) + v(x)·g(x) (7)

ОПРЕДЕЛЕНИЕ. Многочлены f(x) и g(x) называются *взаимно простыми*, если они не имеют других общих делителей кроме многочленов нулевой степени, или, иначе говоря, кроме постоянных из поля *P.*

Многочлены $f_1(x), f_2(x), ..., f_k(x)$ называются *взаимно простыми в совокупности*, если они попарно взаимно просты.

СВОЙСТВО **1.** Многочлены f(x) и g(x), заданные над полем P взаимно просты тогда и только тогда, когда найдутся такие многочлены u(x) и v(x), для которых:

$$u(x)\cdot f(x) + v(x)\cdot g(x) = 1 \qquad (8)$$

СВОЙСТВО **2.** Многочлен g(x) тогда и только тогда взаимно прост с произведением многочленов $f_1(x) \cdot f_2(x) \cdot ... \cdot f_k(x)$, когда он взаимно прост с каждым из сомножителей.

СВОЙСТВО **3.** Если произведение многочленов $f_1(x) \cdot f_2(x)$ делится на многочлен g(x), причем $f_1(x)$ и g(x) взаимно просты, то $f_2(x)$ делится на g(x).

СВОЙСТВО **4.** Если многочлены $f_1(x) \cdot f_2(x) \cdot ... \cdot f_k(x)$ попарно взаимно просты и многочлен f(x) делится на каждый из них, то он делится и на их произведение.

СВОЙСТВО **5.** Многочлены $f_1(x) \cdot f_2(x) \cdot ... \cdot f_k(x)$ взаимно просты тогда и только тогда, когда у них нет корня, общего для всех.

Разложение многочленов на неприводимые множители

ОПРЕДЕЛЕНИЕ. Многочлен p(x) называется *неприводимым над полем P*, если он не раскладывается в произведение двух многочленов положительной степени над эти полем.

ЗАМЕЧАНИЕ. Когда речь идет о неприводимых многочленах, то важно, над каким

полем они рассматриваются, так как один и тот же многочлен может быть неприводим над одним полем и приводим над другим. Например, многочлен f(x) = x^2-3 неприводим над полем рациональных чисел, но приводим над полем действительных чисел, так как f(x) = $(x-\sqrt{3})\cdot(x+\sqrt{3})$ - его разложение в произведение двух многочленов первой степени с действительными коэффициентами.

Отметим свойства неприводимых многочленов, которые выполняются над любым полем P.

СВОЙСТВО **1.** Любой многочлен первый степени неприводим над любым полем.

СВОЙСТВО **2.** Всякий многочлен степени ≥ 2, имеющий корень в поле P, приводим над этим полем.

ЗАМЕЧАНИЕ. Обратное не всегда верно, например, многочлен f(x) = $x^2+2x+1=(x+1)^2$ приводим над полем действительных чисел, хотя не имеет в нем корней.

СВОЙСТВО **3.** Если многочлен *f(x)* ненулевой степени над полем P является делителем неприводимого многочлена *p(x)* над этим же полем, то *f(x)* ассоциирован с *p(x)*: *f(x) = c p(x).*

СВОЙСТВО **4.** Пусть f(x) – произвольный многочлен над полем P и p(x) – неприводимый многочлен над этим же полем. Либо f(x) делится на p(x), либо они взаимно просты.

СВОЙСТВО **5.** Если произведение многочленов $f_1(x)\cdot f_2(x)\cdot\ldots\cdot f_k(x)$ над полем P делится на неприводимый над P многочлен p(x), то хотя бы один из сомножителей делится на p(x).

Из предыдущих параграфов видно, что теория делимости многочленов имеет глубокое сходство с теорией делимости целых чисел. Роль, аналогичную роли простых чисел, играют неприводимые многочлены, что подтверждается следующей теоремой.

ТЕОРЕМА. Каждый многочлен ненулевой степени над полем P может быть представлен и притом единственным образом (с точностью до порядка следования множителей) в виде произведения многочленов, неприводимых над P:

$$f(x)=\alpha\cdot p_1(x)\cdot p_2(x)\cdot\ldots\cdot p_n(x)\ , \qquad (9)$$

где $\alpha\neq 0\in P$, $p_i(x)$, $i\in\{1, 2, \ldots, n\}$ - неприводимые над P многочлены со старшими коэффициентами, равными единице.

ЗАМЕЧАНИЯ

1. Если в разложении (1) собрать вместе одинаковые множители (если таковые имеются) в виде степени, то оно примет вид:

$$f(x) = \alpha\cdot p_1^{k_1}(x)\cdot p_2^{k_2}(x)\cdot\ldots\cdot p_m^{k_m}(x),\ k_i\in N,\ i\in\{1, 2, \ldots, m\}, \quad (10)$$

где все неприводимые множители уже различны между собой.

2. Очевидно, что если для многочленов f(x) и g(x) известны их разложения на неприводимые множители (или такие разложения легко получить), то, как и в случае целых чисел, они могут быть использованы для нахождения НОД и НОК этих многочленов. (Опишите эти алгоритмы самостоятельно).

3. Если говорить об аналогии между кольцом целых чисел и кольцом многочленов от одной переменной, то не следует забывать и о понятии идеала. Например. очевидно, что совокупность всех многочленов кольца P[x], имеющих α своим корнем, будет являться идеалом, причем главным. Порождается этот идеал многочленом наименьшей положительной степени из всех многочленов данной совокупности.

ОПРЕДЕЛЕНИЕ. Для многочлена f(x) = $a_nx^n+a_{n-1}x^{n-1}+\ldots+a_1x+a_0$ будем называть его *производной* f'(x) формальное выражение вида:

$$f'(x) = na_nx^{n-1}+(n-1)a_{n-1}x^{n-2}+\ldots+2a_2x+a_1 \quad (11)$$

ЗАМЕЧАНИЯ

1. Говоря о формальном выражении, мы имеем ввиду, что определение производной многочлена как некоторой функции связано с понятием предела, которое может оказаться неприменимым к элементам произвольного поля P. Поэтому выражение na_n нужно понимать как:

$$\underbrace{a_n + a_n + \ldots + a_n}_{n\ раз} = \underbrace{(1+1+\ldots+1)}_{n\ раз} \cdot a_n . \quad (12)$$

Если в поле P для любого натурального числа k :

$$\underbrace{1+1+\ldots+1}_{k\ раз} \neq 0 ,$$

то соответствующие коэффициенты в выражении (3) не равны нулю и f'(x) можно также считать многочленом над полем P степени n - 1. Поле P со свойством (4) называют *полем нулевой характеристики.*

2. Нетрудно проверить, что для производных многочленов, определенных таким образом, выполняются основные свойства производных функций, а именно:

- числовой множитель можно выносить за знак производной;
- производная суммы многочленов равна сумме их производных;
- производная произведения двух многочленов находится по формуле: (f(x)·g(x))' = f'(x)·g(x) + g'(x)·f(x).

ОПРЕДЕЛЕНИЕ. Производная от производной многочлена f(x) называется его *второй производной* и обозначается как f"(x).

Аналогично определяется и производная k – го порядка $f^{(k)}(x)$.

Найти разложение многочлена f(x) в произведение неприводимых над полем P множителей в общем случае не так просто, как разложение целого числа на простые множители. В этом существенную помощь может оказать введенное понятие производной.

ТЕОРЕМА. Пусть P – поле нулевой характеристики, p(x) – неприводимый делитель многочлена f(x) над P кратности k. В этом случае p(x) будет неприводимым делителем производной многочлена f(x) кратности (k – 1).

В частности, если k = 1, то f'(x) не делится на p(x).

СЛЕДСТВИЕ. Если x_0 - корень кратности k многочлена f(x), то он будет корнем кратности (k – 1) для его производной.

Решим задачу разложения многочлена f(x) на неприводимые множители с помощью последней теоремы.

Пусть разложение f(x) над полем P имеет вид (10). Тогда многочлены $p_1(x), p_2(x), \ldots, p_m(x)$ являются неприводимыми делителями производной f'(x) кратности k_1 -1, k_2 - 1,…, $k_{ü}$ - 1 соответственно.

Отсюда следует, что d(x) = НОД (f(x), f'(x)) имеет вид:

$$d(x) = b \cdot p_1^{k_1-1}(x) \cdot \ldots \cdot p_m^{k_m-1}(x) ,(\ b \neq 0 \in P). \quad (13)$$

Получили, что неприводимые множители d(x) = НОД (f(x), f'(x)) – это в точности кратные неприводимые множители f(x). Для нахождения d(x) можно использовать алгоритм Евклида.

Процедура отыскания НОД (f(x), f'(x)) получила название *отделения кратных неприводимых множителей многочлена f(x)*.

Тема. Расширения полей

План

1. Понятие расширения поля. Алгебраические и трансцендентные числа.

2. Минимальный многочлен алгебраического числа и его свойства.

3. Простое и составное алгебраические расширения.

1. Понятие расширения поля. Алгебраические и трансцендентные числа

ОПРЕДЕЛЕНИЕ. Пусть К и Р – некоторые поля, причем поле К содержится в поле Р: К $\subset$ Р. Тогда К называется *подполем* поля Р, а Р – *надполем* или *расширением* поля К.

Пусть Р есть расширение поля К и α – произвольный элемент поля Р. Очевидно, что существуют поля, которые содержат и поле К, и элемент α. Например, одним из таких полей является само поле Р.

Тогда справедливо УТВЕРЖДЕНИЕ:

Пересечение всех полей, содержащих поле К и элемент α, само является полем, содержащим К и α, которое обозначается как К(α): К $\subseteq$ К(α) $\subseteq$ Р. Очевидно также, что К(α) – наименьшее среди всех подполей поля Р, содержащих поле К и элемент α одновременно.

ЗАМЕЧАНИЕ. Иногда говорят, что элемент α *присоединен* к полю К.

Расширение Р поля К может быть получено присоединением любого конечного (и даже бесконечного) числа элементов $\alpha_1, \alpha_2, \ldots, \alpha_n, \ldots$.

Если расширение получено присоединением одного элемента, то оно называется *простым*.

Так как К(α) – поле, то наряду с элементами поля К и самим элементом α оно, очевидно, содержит всевозможные элементы, получаемые при их сложении, вычитании, умножении и делении.

ТЕОРЕМА. Поле К(α) состоит из рациональных комбинаций элементов из К с элементами, представляющими степени и кратные элемента α.

Пусть дано простое расширение поля К элементом α: К(α).

Тогда оно содержит кольцо всех многочленов от α вида:

$$a_0 + a_1\alpha + a_2\alpha^2 + \ldots + a_n\alpha^n + \ldots, a_k \in K \quad (14)$$

Запишем выражение (1) в виде суммы

$$\sum a_k\alpha^k = f(\alpha) \quad (15)$$

и сравним его с элементами кольца многочленов Ω от одной переменной над тем же полем К – К[x]:

$$f(x) = a_0 + a_1x + a_2x^2 + .. + a_nx^n = \sum a_kx^k \quad (16)$$

Тогда нетрудно проверить, что отображение φ: К[x] $\to \Omega$, заданное следующим образом:

$$\varphi: \sum a_kx^k \to \sum a_k\alpha^k \quad (17)$$

является гомоморфизмом колец.

ЗАМЕЧАНИЯ

1. Из (4) и теоремы о гомоморфизме следует, что кольцо Ω изоморфно фактор-кольцу К[x] / Ker φ, причем ядро гомоморфизма состоит из всех таких многочленов f(x) $\in$ К[x], которые при гомоморфизме φ отображаются в нуль кольца Ω: $\varphi(f(x)) = f(\alpha) = 0_\Omega$,

т.е., оно состоит из таких многочленов, для которых α является корнем. Очевидно, что Ker φ есть идеал в кольце К[x].

Поскольку в кольцах многочленов над полем нет делителей нуля, то идеал Ker φ является простым, т.е. не содержащим собственных идеалов. Он не может быть единичным идеалом, который при гомоморфизме переходит также в единичный идеал, а не в нулевой. Так как в кольце многочленов над полем каждый идеал является главным, то остаются только две возможности.

2. Ker φ = (g(x)), где g(x) – неприводимый над К многочлен. В силу простоты идеала (g(x)), g(x) – многочлен наименьшей степени со свойством g(α) = 0. В этом случае $\Omega \cong$ К[x] / (g(x)).

Кольцо классов вычетов K[x]/(g(x)) является полем (поскольку идеал простой); изоморфное ему кольцо Ω также будет полем, которое в данном случае и является простым расширением кольца K[x].

3. Ker φ = {0}, тогда в кольце K[x] не существует других многочленов, кроме нуля, которые отображались бы в нуль кольца Ω. В этом случае φ является изоморфизмом колец.

4. В случае 2, когда элемент α удовлетворяет некоторому алгебраическому уравнению g(α) = 0 над K, сам элемент α называется *алгебраическим над полем K*, а поле K(α) – *простым алгебраическим расширением* поля K.

В случае 3, когда из равенства f(α) = 0 следует, что f(x) =0, элемент α называется *трансцендентным над* K, а само поле K(α) – *простым трансцендентным расширением* поля K. Очевидно, что во втором случае не существует многочлена с коэффициентами из K, корнем которого являлось бы число α.

Вообще говоря, к понятию алгебраических и трансцендентных чисел подходят обычно следующим образом.

ОПРЕДЕЛЕНИЕ. Число α называется *алгебраическим над полем* P, если оно является корнем какого-либо многочлена с коэффициентами из этого поля. В противном случае число α называется *трансцендентным над полем* P.

ЗАМЕЧАНИЕ. Пусть α есть число, алгебраическое над полем P. Если K есть подполе поля P, то α может уже и не быть алгебраическим над этим полем. Например, число $\alpha = \pi$ будет алгебраическим над полем действительных чисел, так как оно есть корень многочлена f(x) = x - π, но не будет алгебраическим над полем рациональных чисел.

2. Минимальный многочлен алгебраического числа и его свойства

ОПРЕДЕЛЕНИЕ. Поле P называется *конечным расширением поля* K, если любой элемент w $\in$ P является линейной комбинацией конечного числа элементов $u_1, u_2, ..., u_n$ с коэффициентами из поля K*:* $w = a_1u_1 + a_2u_2 + ... + a_nu_n$.

ЗАМЕЧАНИЕ. Очевидно, что поле P можно рассматривать как конечномерное векторное пространство над K. Базисом этого пространства является максимальная линейно независимая подсистема элементов в системе $u_1, u_2, ..., u_n$. Число элементов базиса, т.е. размерность пространства P над K, называется *степенью расширения* P над K и обозначается через [P : K].

Пусть P – простое алгебраическое расширение поля K с помощью элемента α, степень которого над K равна n.

Тогда элементы $1, \alpha, \alpha^2, ..., \alpha^{n-1}$ (18) образуют базис поля P = K(α), т.е. K(α) имеет конечную степень n над K.

Пусть поле L – промежуточное между полями K и P, т.е., K $\subseteq$ L $\subseteq$ P. Тогда справедлива теорема.

ТЕОРЕМА (*о степенях*). Если P конечно над K, то и L конечно над K, а P конечно над L. Обратно, если L конечно над K, а P конечно над L, то P конечно над K, причем

$$[P : K] = [P : L]\cdot[L : K]. \quad (19)$$

ЗАМЕЧАНИЕ. Вторую часть этой теоремы называют также *свойством транзитивности* конечных расширений.

СЛЕДСТВИЕ **1.** Если K $\subseteq$ L $\subseteq$ P и [P : K] = [L : K], то P = L.

СЛЕДСТВИЕ **2.** Если K $\subseteq$ L $\subseteq$ P и [P : L] = [P : K], то L = K.

СЛЕДСТВИЕ **3.** Если K $\subseteq$ L $\subseteq$ P, то степень [L : K] является делителем степени [P : K].

Установим взаимосвязь между расширениями конечной степени и алгебраичностью числа над полем.

ТЕОРЕМА. Число α является алгебраическим над полем P тогда и только тогда, когда векторное пространство P(α) конечномерно над полем P. При этом степень числа α над P равна размерности этого пространства.

СЛЕДСТВИЕ. Пусть К – некоторое кольцо, содержащее поле P. Если пространство К конечномерно над P, то всякое число из кольца *К* алгебраично над P.

ТЕОРЕМА. Совокупность всех чисел, алгебраических над данным полем P, является полем, которое называется *полем алгебраических чисел.*

ОПРЕДЕЛЕНИЕ. Поле называется *алгебраически замкнутым,* если любой многочлен положительной степени с коэффициентами из этого поля имеет корни в этом поле.

Так как любой многочлен с комплексными коэффициентами имеет корень в поле комплексных чисел, то поле С является алгебраически замкнутым.

ТЕОРЕМА. Всякое конечное расширение числового поля является простым алгебраическим расширением этого поля.

Эта теорема означает, что если поле $P(\alpha_1,\alpha_2,...,\alpha_n)$ есть конечное расширение числового поля P, то можно подобрать такое число γ, что $P(\alpha_1,\alpha_2,...,\alpha_n)$ =P(γ).

ОПРЕДЕЛЕНИЕ. Расширение *P* поля К *называется алгебраическим над К*, если каждый элемент из P является алгебраическим над К.

Между конечными и алгебраическими расширениями полей существует тесная взаимосвязь.

ТЕОРЕМА. Каждое конечное расширение поля P алгебраично и получается из P присоединением конечного числа алгебраических элементов.

ЗАМЕЧАНИЕ. Эта теорема позволяет говорить о «конечных алгебраических расширениях» вместо «конечных расширений».

Справедлива и обратная

ТЕОРЕМА. Каждое расширение поля P, которое получается присоединением конечного множества алгебраических чисел к полю P, конечно (и, следовательно, алгебраично).

Для решения некоторых задач полезна следующая

ТЕОРЕМА. Если элемент α алгебраичен над полем P, которое является алгебраическим расширением поля К, то α алгебраичен и над полем К.

Среди всех конечных алгебраических расширений особую роль играют так называемые *поля разложения многочлена* f(x).

ОПРЕДЕЛЕНИЕ. *Полем разложения многочлена* f(x), заданного над полем P, называется поле, полученное присоединением к P всех корней уравнения f(x)=0.

ЗАМЕЧАНИЕ. Речь в определении идет о полях P($\alpha_1,\alpha_2,...,\alpha_n$), в которых многочлен f(x) из кольца P[x] полностью разлагается на линейные множители: f(x)=(x - α_1)·(x - α_2)·…·(x - α_n) и которые получаются присоединением к P корней α_i этих линейных множителей.

В теории полей доказывается

ТЕОРЕМА. Для каждого многочлена f(x) из кольца многочленов P[x] существует некоторое поле разложения.

Тема. Конечные поля

План

1. Строение полей Галуа.

2. Представление элементов поля Галуа конечными числовыми последовательностями и многочленами над конечным полем.

1. Строение полей Галуа

Рассмотрим важный вид полей – конечные поля. Такие поля называются также *полями Галуа* по имени ученого Эвариста Галуа, который первым исследовал их свойства. Поле, содержащее q элементов обозначаю т GF(q).

Так как каждое поле содержит единицу (нейтральный элемент по умножениию) и ноль (нейтральный элемент по сложению), то наименьшее число элементов, образующих поле, равно 2. Такое поле должно содержать только 2 единичных элемента: **0** и **1**.

Это поле GF(2), или двоичное. Правила сложения и умножений для элементов GF(2)приводятся в таблицах на рис 1.

а)

+	0	1
0	0	1
1	1	0

б)

·	0	1
0	0	0
1	0	1

Рис. П1.1

GF(3) –троичное поле с элементами 0, 1, 2. Для него правила сложения и умножения приводятся на рис.2.

а)

+	0	1	2
0	0	1	2
1	1	2	0
2	2	0	1

б)

·	0	1	2
0	0	0	0
1	0	1	2
2	0	2	1

Рис. П1.2

Пусть P – поле Галуа и q – число его элементов. Пусть Π - простое поле, содержащееся в P (напомним, что *простым* называется поле, которое не имеет собственных подполей). Характеристика поля P не может быть нулевой, иначе в простое поле Π также имело бы характеристику нуль, и, следовательно, состояло бы из бесконечного числа элементов.

Пусть p – характеристика данного конечного поля. Тогда простое поле Π изоморфно кольцу классов вычетов кольца целых чисел по mod p и потому содержит p элементов.

Так как поле P конечно, то среди его элементов можно выбрать максимальную систему элементов, линейно независимых над Π:

$$\alpha_1, \alpha_2, ..., \alpha_n .$$

Тогда число n будет степенью расширения [P:П], и каждый элемент из P приобретает вид:

$$c_1\alpha + c_2\alpha_2 + ... + c_n\alpha_n, \qquad (20),$$

где коэффициенты c_i из поля Π однозначно определены.

Так как поле Π содержит ровно p различных элементов, то каждый из коэффициентов в равенстве (1) может принимать p различных значений. Следовательно, имеется в точности p^n выражений вида (1). Поскольку множество всех элементов вида (1) совпадает с множеством всех элементов поля P, то получаем равенство $q = p^n$ (2).

Таким образом, справедлива

ТЕОРЕМА. Число элементов конечного поля является степенью характеристики p; показатель этой степени равен степени расширения [P:П], где Π – простое подполе поля P.

Если выбросить нуль из множества элементов, образующих поле Галуа, то это множество обратится в абелеву мультипликативную группу порядка q - 1. Из свойств

групп следует, что порядок любого элемента α полученной группы должен быть делителем числа q – 1, следовательно,

$$(\forall\ \alpha \in P \setminus \{0\})\ \alpha^{q-1} = 1. \quad (21).$$

Однако, из равенства (3) следует, что уравнение $\alpha^q - \alpha = 0$ имеет своим корнем и $\alpha = 0$.

Таким образом, если рассматривать многочлен $f(x) = x^q - x$, то все элементы поля Галуа будут его корнями.

С другой стороны, если $\alpha_1, \alpha_2, ..., \alpha_q$ - все элементы поля Галуа, то многочлен $f(x) = x^q - x$ делится на многочлен

$$\prod_1^q (x - \alpha_i). \quad (22)$$

В силу равенства степеней многочленов f(x) и (22) получаем их равенство:

$$x^q - x = \prod_1^q (x - \alpha_i). \quad (23).$$

Равенство (23) означает, что поле Галуа P состоит из всех корней многочлена $f(x) = x^q - x$, которые присоединяются к полю Π. Этими условиями поле P определяется однозначно с точностью до изоморфизма. Отсюда следует

ТЕОРЕМА. При заданных числах p и n все поля из p^n элементов изоморфны между собой.

Однако из этой теоремы нельзя сделать выводов о том, для каких чисел p и n существуют поля Галуа. На этот вопрос отвечает

ТЕОРЕМА. Для каждой натуральной степени $q = p^n$ простого числа p ($n > 0$) существует одно и только одно (с точностью до изоморфизма) поле Галуа из q элементов, которые являются корнями многочлена $f(x) = x^q - x$.

Обозначение: поле Галуа из p^n элементов обозначается через $GF(p^n)$.

Преобразуем многочлен $f(x)=x^q - x$ следующим образом:

$$f(x)=x(x^{q-1}-1) \quad (24)$$ и обозначим $q-1=h$.

Тогда все отличные от нуля элементы поля Галуа являются корнями многочлена $x^h - 1$, т.е. корнями h – той степени из единицы. Так как числа h и p взаимно просты, то среди корней h – той степени из единицы существует корень ξ, все различные степени которого совпадают с ненулевыми элементами поля Галуа. Отсюда следует, что $P = \Pi(\xi)$ – простое расширение поля Π. Степень элемента ξ над Π равна степени расширения n.

Приведенные выше рассуждения являются, по существу, доказательством теоремы, которая полностью описывает строение полей Галуа.

ТЕОРЕМА. Мультипликативная группа поля $GF(p^n)$ является циклической группой, порожденной некоторым примитивным (первообразным) корнем h – той степени из единицы.

Следующее свойство позволяет определить все *автоморфизмы* (*изоморфизмы «на себя»*) конечных полей.

СВОЙСТВО. Поле Галуа характеристики p содержит вместе с каждым своим элементом a ровно один корень p – той степени из a.

СЛЕДСТВИЕ. Всеми автоморфизмами поля $GF(p^n)$ являются отображения вида

$$\phi: \alpha \to \alpha^p.$$

Таких отображений будет ровно *n* , и все они есть степени автоморфизма ϕ.

ЗАМЕЧАНИЕ. Нетрудно показать, что все теоремы, справедливые для конечных полей $GF(p^n)$, при n=1 становятся теоремами о кольце вычетов целых чисел по

идеалу, порожденному простым числом p – Z /(p), и приводят к результатам, хорошо известным из теории чисел, например, к таким, как теорема Ферма:

$$a^{p-1} \equiv 1(\text{mod } p),\ a \neq pq,\ q \in Z.$$

2. Представление элементов поля Галуа конечными числовыми последовательностями и многочленами над конечным полем

Рассмотрим теперь возможность построения конечных полей с элементами в виде последовательностей чисел, для чего определим условия, при которых последовательности длины m с элементами из поля GF(q) образуют поле.

Рассмотрим последовательности длины 4 с элементами из GF(2). Такие последовательности можно складывать как векторы, и нулевым элементом по операции сложения является 0000. Для задания операции умножения сопоставим каждой последовательности многочлен от α:

Последовательность	Многочлен
0 0 0 0	0
1 0 0 0	1
0 1 0 0	α
1 1 0 0	$1+\alpha$
0 0 1 0	α^2
1 0 1 0	$1+\alpha^2$
0 0 0 1	α^3
…	…
1 1 1 1	$1+\alpha+\alpha^2+\alpha^3$

Умножение таких многочленов может дать степень, большую чем 3, т.е. последовательность, не принадлежащую рассматриваемому множеству.

Например, $(1101)\cdot(1001) \leftrightarrow (1 + \alpha + \alpha^3)\cdot(1 + \alpha^3) = 1 + \alpha + \alpha^4 + \alpha^6$. Для того чтобы свести ответ к многочлену степени не более 3, положим, что α удовлетворяет уравнению степени 4, например:

$$p(\alpha) = 1 + \alpha + \alpha^4 = 0.$$

Тогда:

$$\alpha^5 = \alpha + \alpha^2,\ \alpha^6 = \alpha^2 + \alpha^3;$$

$$1 + \alpha + \alpha^4 + \alpha^6 = 1 + \alpha + 1 + \alpha + \alpha^2 + \alpha^3 = \alpha^2 + \alpha^3.$$

Это эквивалентно делению на многочлен $1 + \alpha + \alpha^4$ и нахождению остатка от деления:

$$\begin{array}{rll} & \alpha^6+\alpha^4+\alpha+1 & \big|\ \alpha^4+\alpha+1 \\ + & \alpha^6+\alpha^3+\alpha^2 & \big|\ \alpha^2+1 \\ \hline & \alpha^4+\alpha^3+\alpha^2+\alpha+1 & \\ + & \alpha^4+ & \\ \hline & \alpha+1 & \\ \hline & \alpha^3+\alpha^2 - \text{остаток} & \end{array}$$

Таким образом, имеет место аналогия при формировании поля из чисел и последовательностей чисел (или многочленов). Эта аналогия распространяется и на то, что для обратимости введенной операции умножения (чтобы система элементов в виде последовательностей длины m или многочленов степени меньшей m, образовывала поле) многочлен $p(\alpha)$ должен быть неприводим над полем своих коэффициентов.

ОПРЕДЕЛЕНИЕ. Поле, образованное многочленами над полем GF(p) по модулю неприводимого многочлена p(x) степени m, называется *расширением поля степени m*

над GF(p) или *расширенным полем*. Оно содержит p^m элементов и является $GF(p^m)$ – полем, рассмотренным выше.

Поле, образованное шестнадцатью двоичными последовательностями длины 4, или многочленами степени 3 и менее с коэффициентами из GF(2) по модулю многочлена $p(x) = x^4 + x+1$, неприводимого над GF(2), является примером расширенного поля $GF(2^4)$, которое может быть обозначено также GF(16)

Тема. Элементы теории кодирования

План

1. *Задачи теории кодирования, теоремы Шеннона.*
2. *Сжатие информации. Простейшие алгоритмы сжатия.*
3. *Помехоустойчивые коды как пример оптимальных кодов.*

1. Задачи теории кодирования, теоремы Шеннона

Важнейшим разделом теории информации является *теория кодирования*, которая изучает способы отождествления сообщений с отображающими их сигналами.

ОПРЕДЕЛЕНИЕ. Отображение множества состояний источника в множество состояний носителя называется *способом кодирования*, а образ состояния при выбранном способе кодирования – *кодом* этого состояния.

Задачей теории кодирования является наилучшее в некотором смысле согласование источника информации с каналом связи (например, обеспечение максимальной скорости передачи для заданных статистических характеристик сообщений либо обеспечение заданной помехоустойчивости при заданных характеристиках помех в канале, либо обеспечение максимальной скорости переработки информации при арифметических операциях). В соответствии с принятым критерием оптимизации различают несколько направлений в теории кодирования. Наиболее известными из них являются - статистическое кодирование и помехоустойчивое кодирование. Объектами кодирования могут быть как дискретные, так и непрерывные сообщения.

К.Шеннон сформулировал и доказал два основных результата.

ТЕОРЕМА **1.** Для случая канала без помех возможно осуществить кодирование дискретных сообщений таким образом, чтобы среднее количество двоичных знаков на элемент исходного алфавита было как угодно близко, но не менее некоторой величины - энтропии источника информации, определяемой статистическими свойствами источника. Такое кодирование получило название статистического (эффективного).

ТЕОРЕМА **2.** Для канала связи с шумами существует такой способ кодирования конечного количества информации, при котором информация будет передана с какой угодно высокой достоверностью, если только скорость поступления ее не превышает пропускную способность канала связи.

ЗАМЕЧАНИЕ. Реализация этой возможности неразрывно связана с теорией и техникой кодов корректирующих и помехоустойчивых методов приема. Теоремы Шеннона устанавливают только существование оптимальных или близких к ним кодов, но не указывают способа построения их.

В общем случае условия основных теорем Шеннона выполняются лишь при увеличении длины кодируемых сообщений до бесконечности. Исследования в области теории кодирования ведутся в основном в направлении обоснования и разбора условий основных теорем Шеннона и в направлении создания наилучших методов кодирования информации.

2. Сжатие информации. Простейшие алгоритмы сжатия

Применение сжатия данных позволяет более эффективно использовать емкость дисковой памяти. Не менее полезно применение сжатия при передаче информации в любых системах связи. В последнем случае появляется возможность передавать значительно меньшие (как правило, в несколько раз) объемы данных и, следовательно, требуются значительно меньшие ресурсы пропускной способности каналов для

передачи той же самой информации. Выигрыш может выражаться в сокращении времени занятия канала и, соответственно, в значительной экономии арендной платы.

Сжатие данных – подраздел теории информации, близко соприкасающийся с теорией кодирования, поскольку любые методы сжатия данных основаны на поиске избыточной информации и последующем ее кодировании с целью получения минимального объема. По существу, сжатие данных – это кодирование источника, которое приводит к уменьшению числа символов в сообщении до минимума, необходимого для представления всей информации сообщения или, по крайней мере, для обеспечения условий такого сообщения.

Существуют два основных класса методов сжатия информации:

1) класс методов необратимого сжатия, имеющих также название энтропийного сжатия, или сжатия с потерями,

2) класс методов обратимого – восстановимого преобразования исходной информации.

Б.М. Фитингоф, Р.Е. Кричевский, Ю.М. Штарьков и другие рассмотрели случайные последовательности с неизвестным заранее распределением вероятностей и разработали оптимальные для бесконечных последовательностей методы описания на основе наблюдения статистики первых символов последовательности. Это направление получило название оптимального универсального кодирования. Хорошие результаты по сжатию можно получить только для определенного источника на основе точного знания его свойств.

Научной предпосылкой возможности сжатия данных выступает известная из теории информации теорема кодирования Шеннона для канала без помех.

Для характеристики достижимой степени сжатия используется коэффициент избыточности (КИЗБ).

Для характеристики же достигнутой степени сжатия на практике применяют так называемый коэффициент сжатия, который выражает отношение первоначального размера данных к их размеру в сжатом виде. Известные методы сжатия направлены на снижение избыточности, вызванной как неравной вероятностью символов, так и зависимостью между порядком их поступления. В первом случае для кодирования исходных символов используется *неравномерный код*. Часто появляющиеся символы кодируются более коротким кодом, а менее вероятные (редко встречающиеся) — более длинным кодом.

Существуют два основных способа проведения сжатия: статистический и словарный. Лучшие статистические методы применяют арифметическое кодирование, лучшие словарные – метод Зива-Лемпела. В статистическом сжатии каждому символу присваивается код, основанный на вероятности его появления в тексте. Высоковероятные символы получают короткие коды, и наоборот. В словарном методе группы последовательных символов или "фраз" заменяются кодом. Замененная фраза может быть найдена в некотором "словаре". Только в последнее время было показано, что любая практическая схема словарного сжатия может быть сведена к соответствующей статистической схеме сжатия, и найден общий алгоритм преобразования словарного метода в статистический. Поэтому при поиске лучшего сжатия статистическое кодирование обещает быть наиболее плодотворным, хотя словарные методы и привлекательны своей быстротой.

В основе вероятностных методов сжатия (алгоритмов *Шеннона-Фано* и *Хаффмена*) лежит идея построения "дерева", положение символа на "ветвях" которого определяется частотой его появления. Каждому символу присваивается код, длина которого обратно пропорциональна частоте появления этого символа. Существуют две разновидности вероятностных методов, различающихся способом определения вероятности появления каждого символа:

- статические методы, использующие фиксированную таблицу частоты появления символов, рассчитываемую перед началом процесса сжатия;

- динамические или адаптивные методы, в которых частота появления символов все время меняется и по мере считывания нового блока данных происходит перерасчет начальных значений частот.

Статические методы характеризуются хорошим быстродействием и не требуют значительных ресурсов оперативной памяти. Они нашли широкое применение в многочисленных программах-архиваторах, например ARC, PKZIP и др., но для сжатия передаваемых модемами данных используются редко — предпочтение отдается арифметическому кодированию и методу словарей, обеспечивающим большую степень сжатия.

Арифметическое кодирование

Принципы арифметического кодирования были разработаны в конце 70-х годов. В результате арифметического кодирования строка символов заменяется действительным числом больше нуля и меньше единицы. Арифметическое кодирование позволяет обеспечить высокую степень сжатия, особенно в случаях, когда сжимаются данные, где частота появления различных символов сильно варьируется. Однако сама процедура арифметического кодирования требует мощных вычислительных ресурсов, и до недавнего времени этот метод мало применялся при сжатии передаваемых данных из-за медленной работы алгоритма. Лишь появление мощных процессоров, особенно с RISC-архитектурой, позволило создать эффективные устройства арифметического сжатия данных.

Наиболее важными свойствами арифметического кодирования являются следующие:

- способность кодирования символа вероятности p количеством битов произвольно близким к -log p;
- вероятности символов могут быть на каждом шаге различными;
- очень незначительный запрос памяти независимо от количества классов условий в модели;
- большая скорость.

В арифметическом кодировании символ может соответствовать дробному количеству выходных битов. В нашем примере, в случае появления буквы "о" он может добавить к нему 0.014 бита. На практике результат должен, конечно, являться целым числом битов, что произойдет, если несколько последовательных высоко вероятных символов кодировать вместе, пока в выходной поток нельзя будет добавить 1 бит. Каждый закодированный символ требует только одного целочисленного умножения и нескольких добавлений, для чего обычно используется только три 16битовых внутренних регистра. Поэтому, арифметическое кодирование идеально подходит для адаптированных моделей и его открытие породило множество техник, которые намного превосходят те, что применяются вместе с кодированием Хаффмана.

Сложность арифметического кодирования состоит в том, что оно работает с накапливаемой вероятностью распределения, требующей внесения для символов некоторой упорядоченности. Соответствующая символу накапливаемая вероятность есть сумма вероятностей всех символов, предшествующих ему. Эффективная техника организации такого распределения приводится в [115]. В [68] дается эффективный алгоритм, основанный на двоичной куче для случая очень большого алфавита, другой алгоритм, основанный на расширяющихся деревьях, дается в [47]. Оба они имеют приблизительно схожие характеристики.

Методы Шеннона-Фано и Хаффмена

В качестве примера, поясняющего принципы сжатия, рассмотрим простой метод Шеннона-Фано. Согласно этому методу, для каждого символа формируется битовый код, причем символы с различными частотами появления имеют коды разной длины. Чем меньше частота появления символов в файле, тем больше размер его битового кода. Соответственно, чаще появляющийся символ имеет меньший размер кода.

Код строится следующим образом: все символы, встречающиеся в файле, выписывают в таблицу в порядке убывания частот их появления. Затем их разделяют на две группы так, чтобы в каждой из них были примерно равные суммы частот символов. Первые биты кодов всех символов одной половины обозначаются "0", а второй — в "1". После этого каждую группу делят еще раз пополам и так до тех пор, пока в каждой группе не останется по одному символу.

Однако данный способ не всегда приводит к построению однозначного кода. Хотя в верхней подгруппе средняя вероятность символа больше (и, следовательно, коды должны быть короче), возможны ситуации, при которых программа сделает длиннее коды некоторых символов из верхних подгрупп, а не коды символов из нижних подгрупп. Действительно, разделяя множество символов на подгруппы, можно сделать большей по вероятности как верхнюю, так и нижнюю подгруппы.

Более удачен в данном отношении метод Хаффмена. Он позволяет однозначно построить код с наименьшей средней длиной, приходящейся на символ. Суть метода Хаффмена сводится к следующему. Символы, встречающиеся в файле, выписываются в столбец в порядке убывания вероятностей (частоты) их появления. Два последних символа объединяются в один с суммарной вероятностью. Из полученной новой вероятности и вероятностей новых символов, не использованных в объединении, формируется новый столбец в порядке убывания вероятностей, а две последние вновь объединяются. Это продолжается до тех пор, пока не останется одна вероятность, равная сумме вероятностей всех символов, встречающихся в файле. Для составления кода, соответствующего данному символу, необходимо проследить путь перехода знака по строкам и столбцам таблицы кода.

3. Помехоустойчивые коды как пример оптимальных кодов

Проблема повышения верности обусловлена несоответствием между требованиями, предъявляемыми при передаче данных, и качеством реальных каналов связи. В сетях передачи данных требуется обеспечить верность не хуже 10^{-6} - 10^{-9}, а при использовании реальных каналов связи и простого (первичного) кода указанная верность не превышает 10^{-2} - 10^{-5}. Одним из путей решения задачи повышения верности в настоящее время является использование специальных процедур, основанных на применении *помехоустойчивых* (*корректирующих*) кодов.

Простые коды характеризуются тем, что для передачи информации используются все кодовые слова (комбинации), количество которых равно $N=q^n$ (q – основание кода, а n – длина кода). В общем случае они могут отличаться друг от друга одним символом (элементом). Поэтому даже один ошибочно принятый символ приводит к замене одного кодового слова другим и, следовательно, к неправильному приему сообщения в целом.

Помехоустойчивыми называются коды, позволяющие обнаруживать и (или) исправлять ошибки в кодовых словах, которые возникают при передаче по каналам связи. Эти коды строятся таким образом, что для передачи сообщения используется лишь часть кодовых слов, которые отличаются друг от друга более чем в одном символе. Эти кодовые слова называются разрешенными. Все остальные кодовые слова не используются и относятся к числу запрещенных.

Применение помехоустойчивых кодов для повышения верности передачи данных связанно с решением задач кодирования и декодирования.

Задача кодирования заключается в получении при передаче для каждой k - элементной комбинации из множества q^k соответствующего ей кодового слова длиною n из множества q^n.

Задача декодирования состоит в получении k - элементной комбинации из принятого n – разрядного кодового слова при одновременном обнаружении или исправлении ошибок.

К основным параметрам помехоустойчивых кодов относятся следующие величины:

- длина кода – n;
- длина информационной последовательности – k;
- длина проверочной последовательности – r=n-k;
- кодовое расстояние кода – d_0.

ОПРЕДЕЛЕНИЕ. *Кодовым расстоянием* между двумя кодовыми словами (расстояние Хэмминга) называется число позиций, в которых они отличаются друг от друга.

Кодовым расстоянием кода называется наименьшее расстояние Хэмминга между различными парами кодовых слов. *Стиранием* называется "потеря" значения передаваемого символа в некоторой позиции кодового слова, которая известна.

ОПРЕДЕЛЕНИЕ. Код, в котором каждое кодовое слово начинается с информационных символов и заканчивается проверочными символами, называется *систематическим.*

Одной из важнейших задач построения помехоустойчивых кодов с заданными характеристиками является установление соотношения между его способностью обнаруживать или исправлять ошибки и избыточностью. Подобные соотношения получили название *граничных соотношений* между параметрами помехоустойчивых кодов.

Линейные блоковые коды

ОПРЕДЕЛЕНИЕ. *Линейным блоковым (n, k) - кодом* называется множество N последовательностей длины n над конечным полем GF(q), называемых кодовыми словами, которое характеризуется тем, что сумма двух кодовых слов является кодовым словом, а произведение любого кодового слова на элемент поля также является кодовым словом. Обычно $N=q^k$, где k - некоторое целое число.

ЗАМЕЧАНИЕ. Напомним, что обозначение GF(q) используется для конечного поля характеристики q, т.е. такого поля, в котором выполняется равенство:

$$\underbrace{1_P + 1_P + \ldots + 1_P}_{q\ раз} = 0 .$$

ОПРЕДЕЛЕНИЕ. Если q=2, линейные коды называются *групповыми*, так как кодовые слова образуют математическую структуру, называемую группой.

При формировании этого кода линейной операцией является суммирование по mod 2.

Назовем основные способы задания линейных кодов.

1. Перечисление кодовых слов

Этот способ заключается в составлении списка всех кодовых слов кода.

2. Система проверочных уравнений

Системы проверочных уравнений определяют правила формирования проверочных символов по известным информационным:

$$b_j = \sum_{i=1}^{k} a_i \cdot h_{ij},$$

где: j – номер проверочного символа; i – номер информационного символа; h_{ij} – коэффициенты, принимающие значения 0 или 1 в соответствии с правилами формирования конкретных групповых кодов.

3. Матричный

Этот способ основан на построении *порождающей* и *проверочной* матриц.

Векторное пространство Vn над полем GF(2) включает в себя 2^n векторов (n-последовательностей), а подпространством его является множество из 2^k кодовых слов длины n, которое однозначно определяется его базисом, состоящим из k линейно независимых векторов. Поэтому линейный (n, k) - код полностью определяется набором из k кодовых слов, принадлежащих этому коду. Набор из k кодовых слов, соответствующих базису, обычно представляется в виде матрицы, которая называется порождающей.

Остальные кодовые слова получаются сложением строк матриц в различных сочетаниях. Общее количество различных вариантов, порождающих матрицу, определяется выражением

$$M_{(n,k)} = \prod_{i-0}^{k-1}\left(2^k - 2^i.\right)$$

Для исключения неоднозначности в записи G(n,k) вводят понятие о канонической или систематической форме матрицы, которая имеет вид:

$$G_{(n,k)} = \left(I_k, R_{k,r}\right),$$

где: I_k – единичная матрица, содержащая информационные символы; $R_{k,r}$ – прямоугольная матрица, составленная из проверочных символов.

Порождающая матрица $G_{(n,k)}$ в систематическом виде может быть получена из любой другой матрицы посредством элементарных операций над строками (перестановкой двух произвольных строк, заменой произвольной строки на сумму ее самой и ряда других) и дальнейшей перестановкой столбцов.

Проверочная матрица в систематическом виде имеет вид:

$$H_{(n,k)} = \left(R^T{}_{k,r}, I_r,\right),$$

где I_r – единичная матрица; $R^T{}_{k,r}$ – прямоугольная матрица в транспонированном виде матрицы $R_{k,r}$ из порождающей матрицы.

Отметим основные свойства линейных кодов.

СВОЙСТВО 1. Произведение любого кодового слова $v_i(x)$ на транспонированную проверочную матрицу дает нулевой вектор размерности (n-k):

$$v_i(x)\cdot H^T_{(n,k)} = (00\ldots).$$

ОПРЕДЕЛЕНИЕ. Произведение некоторого кодового слова $v_i^{'}(x)$, т.е. с ошибкой, на транспонированную проверочную матрицу называется *синдромом* и обозначается $S_i(x)$:

$$v_i'(x)\cdot H^T_{(n,k)} = S_i(x).$$

СВОЙСТВО 2. Между порождающей и проверочной матрицами в систематическом виде существует однозначное соответствие, а именно:

$$G_{(n,k)}\cdot H^T_{(n,k)} = 0\,.$$

СВОЙСТВО 3. Кодовое расстояние d_0 (n,k) кода равно минимальному числу линейно зависимых столбцов проверочной матрицы.

СВОЙСТВО 4. Произведение информационного слова на порождающую матрицу дает кодовое слово кода.

ОПРЕДЕЛЕНИЕ. Два кода называются *эквивалентными*, если их порождающие матрицы отличаются перестановкой координат, т.е. порождающие матрицы получаются одна за другой перестановкой столбцов и элементарных операций над строками.

Стандартное расположение группового кода

Стандартное расположение группового кода представляет собой разложение множества всех возможных n-элементных слов, представляющих собой группу, на смежные классы по подгруппе из 2^k кодовых слов, составляющих (n, k)-код (таблица 1).

Таблица 1. Стандартное расположение группового кода.

$v_0(x)$	$v_1(x)$	…	$v_i(x)$	…	$v_{2^{k-1}}(x)$
$l_1(x)$	$v_1(x)+l_1(x)$	…	$v_i(x)+l_1(x)$	…	$v_{2^{k-1}}(x)+l_1(x)$

⋮	⋮	…	⋮	…	⋮
$l_j(x)$	$v_1(x)+l_j(x)$	…	$v_i(x)+l_j(x)$	…	$v_{2^{k-1}}(x)+l_j(x)$
⋮	⋮	…	⋮	…	⋮
$l_{2^{r-1}}(x)$	$v_1(x)+l_{2^{r-1}}(x)$	…	$v_i(x)+l_{2^{r-1}}(x)$	…	$v_{2^{k-1}}(x)+l_{2^{r-1}}(x)$

Образующие или *лидеры* смежных классов выбираются таким образом, чтобы в их состав вошли наиболее вероятные образцы ошибок в кодовом слове, т.е. образцы ошибок с наименьшим весом.

ОПРЕДЕЛЕНИЕ. *Кодом Хэмминга* называется (n, k)-код, проверочная матрица которого имеет r=n-k строк и 2^r-1 столбцов, причем столбцами являются все различные ненулевые последовательности.

Проверочная матрица любого кода Хэмминга всегда содержит минимум три линейно зависимых столбца, поэтому кодовое расстояние кода равно трем.

Если столбцы проверочной матрицы представляют упорядоченную запись десятичных чисел, т.е. 1,2,3... в двоичной форме, то вычисленный синдром

$$S_i(1,0) = S_{r-1}\ldots S_1 S_0 = v_i(1,0)\cdot H^T_{(n,k)}$$

однозначно указывает на номер позиции искаженного символа.

Циклические коды

ОПРЕДЕЛЕНИЕ. *Циклическим кодом* называется линейный блоковый (n, k)-код, который характеризуется свойством цикличности, т.е. сдвиг влево на один шаг любого разрешенного кодового слова дает также разрешенное кодовое слово, принадлежащее этому же коду, и у которого множество кодовых слов представляется совокупностью многочленов степени (n - 1) и менее, делящихся на некоторый многочлен g(x) степени r=n-k, являющийся сомножителем двучлена x^{n+1}. Многочлен g(x) называется *порождающим*.

Как следует из определения, в циклическом коде кодовые слова представляются многочленами вида:

$$v(x) = v_{n-1}\cdot x^{n-1} + v_{n-2}\cdot x^{n-2} + \cdots + v_1\cdot x^1 + v_0\cdot x^0$$

где n – длина кода; v_i – коэффициенты из поля GF(q).

Если код построен над полем GF(2), то коэффициенты принимают значения 0 или 1 и код называется двоичным.

ОПРЕДЕЛЕНИЕ. Длина циклического кода называется *примитивной* и сам код называется *примитивным*, если его длина $n = q^m - 1$ над GF(q).

Если длина кода меньше длины примитивного кода, то код называется *укороченным* или *непримитивным*.

Общее свойство кодовых слов циклического кода - это их делимость без остатка на некоторый многочлен g(x), называемый порождающим.

Результатом деления двучлена $x^n + 1$ на многочлен g(x) является проверочный многочлен h(x).

При декодировании циклических кодов используются *многочлен ошибок e(x)* и *синдромный многочлен S(x).*

Многочлен ошибок, степени не более (n - 1) определяется из выражения

$$e(x) = v'(x) + v(x),$$

где *v(x)* и *v′(x)* - многочлены, отображающие соответственно принятое (с ошибкой) и переданное кодовые слова.

Ненулевые коэффициенты в e(x) занимают позиции, которые соответствуют ошибкам.

Матричное задание кодов

Циклический код может быть задан порождающей и проверочной матрицами. Для их построения достаточно знать порождающий g(x) и проверочный h(x) многочлены.

Для несистематического циклического кода матрицы строятся циклическим сдвигом порождающего и проверочного многочленов, т.е. путем их умножения на x:

$$G_{(n,k)} = \begin{pmatrix} g(x) \\ x \cdot g(x) \\ x^2 \cdot g(x) \\ \cdots\cdots\cdots \\ x^{k-1} \cdot g(x) \end{pmatrix}, \quad H_{(n,k)} = \begin{pmatrix} h(x) \\ x \cdot h(x) \\ x^2 \cdot h(x) \\ \cdots\cdots\cdots \\ x^{r-1} \cdot h(x) \end{pmatrix}.$$

При построении матрицы $H_{(n,k)}$ старший коэффициент многочлена h(x) располагается справа.

Одна из основных задач, стоящих перед разработчиками устройств защиты от ошибок при передаче дискретных сообщений по каналам связи, - это выбор порождающего многочлена g(x) для построения циклического кода, обеспечивающего требуемое минимальное кодовое расстояние для гарантийного обнаружения и исправления t-кратных ошибок.

Существуют специальные таблицы по выбору g(x) в зависимости от предъявляемых требований к корректирующим возможностям кода. Однако у каждого циклического кода имеются свои особенности формирования g(x). Поэтому при изучении конкретных циклических кодов будут рассматриваться соответствующие способы построения g(x).

Методические материалы для обучающихся по подготовке к практическим занятиям

Тема. Алгебраические системы

План

1. Отношения эквивалентности. Отношения порядка. Разбиения множества.

2. Понятие и свойства бинарной алгебраической операции.

3. Группы. Нормальные делители. Кольца и поля.

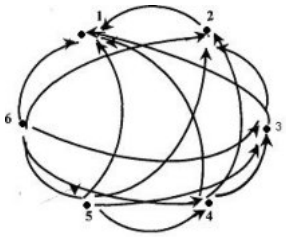
1. Отношения эквивалентности. Отношения порядка. Разбиения множества

Задание 1. Дано множество *A*={1;2;3;4;5;6}. На нем задано бинарное отношение ρ «больше», т. е. $< x, y > \in \rho \Leftrightarrow x > y$.

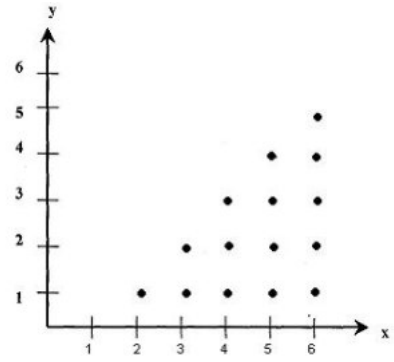
Построить граф и график этого отношения. Какими свойствами обладает это отношение?

Решение.

1) Граф указанного отношения:



2) График этого отношения:



3) Рефлексивность. Если бы это отношение было рефлексивным, $(\forall x \in A)\, x > x$, например, было бы верно 2 > 2 (ложь). Значит отношение «>» на *A* не является рефлексивным.

Симметричность. Если бы это отношение было симметричным на множестве *A*, то $(\forall x, y \in A)(x > y \Rightarrow y > x)$. Например, 3 > 2 => 2 > 3(ложь). Значит, отношение « > » на *A* не является симметричным.

Транзитивность. Если бы это отношение было транзитивным на множестве *A*, то $(\forall x, y, z \in A)(x > y \wedge y > z \Rightarrow x > z)$. Это утверждение истинно для любых натуральных чисел, т. е. и для чисел из *A*. Значит, отношение « > » на *A* является транзитивным.

Асимметричность: Ни для каких чисел *A* не может быть одновременно истинным

$$\begin{cases} x > y \\ y > x \end{cases},$$

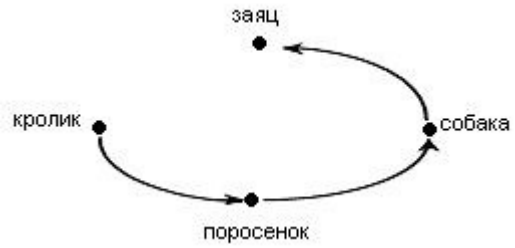
т.е. отношение «>» на *A* асимметрично. Отношение «>» на множестве *A* является отношением строгого порядка, т. к. оно асимметрично и транзитивно.

Т.к. отношение «>» на множестве *A* связное и является отношением строгого порядка, то оно есть отношение строгого линейного порядка.

Задание 2. Построить граф отношения «легче, чем» на множестве *A* = {кролик, заяц, собака, поросёнок}, если известно, что заяц тяжелее собаки, кролик легче поросёнка, а собака тяжелее поросёнка. Кто из животных самый легкий, кто – самый тяжелый.

Решение.

Строим граф указанного отношения:



Ответ: кролик – самый легкий, заяц – самый тяжелый.

На множестве людей Земли введено бинарное отношение «быть родственником по крови». Будет ли это отношение отношением эквивалентности?

Решение.

Задание 3. Обозначим через *A* множество людей Земли, а заданное отношение буквой ρ. Тогда *x*ρ*y* <=> человек *x* является родственником человека *y*. Что бы отношение ρ было отношением эквивалентности, оно должно быть рефлексивным, симметричным, транзитивным.

Рефлексивность. Если бы ρ было рефлексивным, то было бы верно: $(\forall x \in A)$ $x\rho x$, т. е. любой человек Земли является родственником самому себе (истина), т.е. отношение ρ на *A* рефлексивно.

Симметричность. Если бы ρ было симметрично. ($x\rho y$ => $y\rho x$), т. е. если бы человек *x* был родственником человека *y*, то *y* был бы родственником человека *x* (истина). Значит, отношение ρ на *A* симметрично.

Транзитивность. Если бы ρ было транзитивно на *A*, то если бы человек *x* был бы родственником человека *y*, а *y* был родственником человека *z*, то *x* был бы родственником *z*. Но это не обязательно. Например, человек *x* родственник для *y* по матери, а *y* – родственник для *z* по отцу. Тогда *x* и *y* могут не быть родственниками по крови. Значит, отношение ρ на *A* не является транзитивным.

Следовательно, отношение «быть родственником по крови» на множестве людей Земли не является отношением эквивалентности.

Задание 4. Сформулировать свойства отношения «больше в 2 раза», заданного на множестве натуральных чисел.

Решение.

«Больше в 2 раза» – это краткая запись отношения «число x больше числа y в 2 раза».

Это отношение антисимметрично, так как выполняется условие: из того, что число x больше числа y в 2 раза, следует, что число y не больше числа x в 2 раза.

Данное отношение не обладает свойством рефлексивности, потому что ни про одно число нельзя сказать, что оно больше самого себя в 2 раза.

Заданное отношение не транзитивно, так как из того, что число x больше числа y в 2 раза, а число y больше числа z в 2 раза, следует, что число x не может быть больше числа z в 2 раза.

Это отношение на множестве натуральных чисел свойством связности не обладает, так как существуют пары таких чисел x и y, что ни число x не больше числа y в два раза, ни число y не больше x в 2 раза. Например, это числа 7 и 3, 5 и 8 и др.

Задания

1. На множестве $A = \{1; 5; 7\}$ задано бинарное отношение $\rho = \{(1;1), (1;7), (5;1), (5;5), (7;5)\}$. 1) Найти $\rho^{-1}; \overline{\rho}; \overline{\rho}^{-1}$; 2) начертить граф и график бинарного отношения ρ.

2. На множестве задано бинарное отношение с помощью графика. Определить, какими свойствами оно обладает. Добавить одну точку так, чтобы бинарное отношение стало рефлексивным. Добавить две точки так, чтобы оно стало транзитивным.

3. На множестве натуральных чисел задано бинарное отношение ρ следующим образом: $x \rho y \Leftrightarrow |y - x| = 12$. Определить, какими свойствами оно обладает.

4. Для следующего бинарного отношения, определённого на множестве натуральных чисел, найти область определения, область значений, указать свойства и нарисовать график: $x \rho y \Leftrightarrow x = 3y$.

5. Указать свойства бинарного отношения ρ, если ρ - это отношение «работать на одной кафедре» во множестве преподавателей и сотрудников института.

6. Определить, является ли следующее бинарное отношение отображением. Если да, то является ли оно инъекцией, сюръекцией, биекцией? а) $\varphi = \{(x;y) \in R \times R \mid y = x^2\}$, б) $f = \{(x;y) \in N \times N \mid x - y = 3\}$.

7. Выяснить, является ли данное отображение инъективным, сюръективным: $f : R \to R,\ x \to \log_2\left(x^2 + \frac{1}{2}\right)$.

8. Дано множество $A=\{1;2;3;4\}$; $A_1=\{1;2\}, A_2=\{3\}, A_3=\{4\}$ - разбиение этого множества на классы. Построить по данному разбиению отношение эквивалентности.

9. Доказать, что $\sigma=\{(a;a);(b;b);(c;c);(d;d);(c;d);(d;c);(a;b);(b;a)\}$ является отношением эквивалентности и построить по нему разбиение множества $A=\{a,b,c,d\}$ на классы.

10. На множестве целых чисел задано бинарное отношение ρ следующим образом: $x\rho y \Leftrightarrow (x-y)\vdots 7$. Доказать, что ρ – отношение эквивалентности, и построить разбиение на классы по данному отношению эквивалентности.

11. Построить разбиение на классы по отношению равенства на множестве Z, предварительно убедившись, что оно является отношением эквивалентности.

12. M – множество городов планеты Земля, ρ – отношение «город x расположен в том же государстве, что и город y». Доказать, что ρ является отношением эквивалентности, и построить по нему разбиение множества M на классы.

13. Дано множество $A=\{a,b,c\}$. Сколько можно задать на нём разных отношений эквивалентности?

2. Понятие и свойства бинарной алгебраической операции

Задание 1. Примерами бинарных операций, заданных на числовых множествах, могут служить операции обычного сложения и умножения чисел, примерами унарных операций – взятие обратного и противоположного элементов, возведение в степень или извлечение корня, примерами нульарных операций - выделение нуля или единицы.

Задание 2. Множество N натуральных чисел по операции обычного умножения образует абелев моноид <N, • >.

Множество N по операции обычного сложения также образует абелев моноид <N, + >, так как:

$$(\forall a, b \in N) \quad a + b \in N;$$
$$(\forall a, b, c \in N) \quad a + (b + c) = (a + b) + c;$$
$$(\forall a, b \in N) \quad a + b = b + a;$$
$$(\forall a \in N) \quad a + 0 = 0 + a = a;$$

однако операция сложения не обратима на N, так как, например, для числа 2 не существует обратного (противоположного) элемента в множестве N.

Так как $(\forall a, b, c \in N)$ $c\cdot(a + b) = c\cdot a + c\cdot b$, то умножение на N дистрибутивно относительно сложения.

Из сказанного следует, что структура <N, +, • > образует ассоциативно-коммутативное полукольцо с единицей.

Задание 3.

1). Операция обычного сложения на множестве всех целых чисел *Z:*

- ассоциативна, т.к. $(\forall a, b, c \in Z)$ $a +(b + c) = (a + b) + c$;
- коммутативна, т.к. $(\forall a, b \in Z)$ $a + b = b + a$;
- обладает двусторонним нейтральным элементом, роль которого играет целое число 0*:* $(\exists 0 \in Z)$ $(\forall a \in Z)$ $a + 0 = 0 + a = a$;
- обратима, т.к. $(\forall a \in Z)$ $(\exists - a \in Z)$ $-a + a = a + (-a) = 0$;
- двусторонне сократима, т.к. $(\forall a, b, c \in Z)$ $(a + c = b + c \Rightarrow a = b)$.

2). Операция обычного умножения на множестве всех целых чисел *Z* дистрибутивна относительно операции сложения, так как:

$$(\forall a, b, c \in Z) \quad c(a + b) = ca + cb \text{ и}$$
$$(\forall a, b, c \in Z) \quad (a + b)c = ac + bc.$$

Задания

1. Выяснить, какими свойствами обладают следующие бинарные операции, заданные на указанных множествах:

2. $A = R, (\forall a,b \in R)\, a \circ b = \frac{a+b}{2}$;

3. $A = R^+, a \circ b = a^b$;

4. $A = N, a * b = \max\{a; b\}$.

5. Определить, какой алгебраической структурой является множество A по операции умножения, если: а) $A = \{2^n \mid n \in Z\}$, б) $A = \{x + y\sqrt{3} \mid x, y \in R\}$.

6. Являются ли алгебраическими следующие числовые операции:
   a. операция деления на множестве Q;
   b. операция деления на множестве Z;
   c. операция вычитания на множестве Z;
   d. операция вычитания на множестве N;
   e. операция извлечения корня на множестве R;
   f. операция извлечения корня на множестве A = {x∈R, x > 1};
   g. операция извлечения корня на множестве A = {x∈R, x > 2}?

7. В группе из четырех подростков: Саши, Даши, Пети и Маши взаимоотношения определяются следующими условиями:
   a. У Саши и Даши авторитет Даша.
   b. У Саши и Маши авторитет Саша.
   c. У Саши авторитет Саша.
   d. У Даши и Маши авторитет Саша.
   e. У Даши авторитет Даша.
   f. У Маши авторитет Петя.
   g. У Пети и Даши авторитет Петя.
   h. У Пети и Маши авторитет Петя.
   i. У Пети и Саши авторитет Саша.
   j. У Пети авторитет Саша.

8. Можно ли утверждать, что на множестве из четырех человек задана бинарная алгебраическая операция? Каковы ее свойства?

9. Какую структуру образует множество A по операции «*»:
   a. A = R^+; x*y = $\frac{x+y}{2}$.
   b. A = Z; x*y = x + y – 1.
   c. A = Q; x*y = $\sqrt{xy}$.
   d. A = N; x*y = 1.
   e. A = R; x*y = xy^2.
   f. A = {a +b$\sqrt{3}$ | a, b ∈Q, $a^2 + b^2 \neq 0$}; операция «*» - операция обычного сложения чисел.
   g. A = {a +b$\sqrt{5}$ | a, b ∈Q, $a^2 + b^2 \neq 0$}; операция «*» - операция обычного умножения чисел.
   h. A = {$\frac{a}{7^k}$ | a ∈Z, k ∈N}; операция «*» - операция обычного сложения чисел.
   i. A = N; x*y = max{x, y}.
   j. A = Z; x*y = |x – y|.

3. Группы. Нормальные делители. Кольца и поля

Задание 1. Аддитивная группа всех целых чисел изоморфна своей подгруппе, состоящей из четных чисел, так как отображение φ: Z → 2Z такое, что:

(∀ x ∈ Z) $\varphi(x) = 2x$,

является изоморфизмом групп, так как очевидно, что φ - биективно и ($\forall$ x, y $\in$ Z) φ(x + y) = 2(x +y) = 2x + 2y = φ(x) + φ(y).

Задание 2. Аддитивная группа всех действительных чисел изоморфна мультипликативной группе всех положительных действительных чисел:

$$<R, + > \cong <R^+, \bullet >,$$

так как отображение φ: R $\rightarrow$ R^+, при котором:

$$(\forall x \in R) \quad \varphi(x) = e^x$$

является биекцией, поскольку:

$$(\forall x, y \in R) \quad \varphi(x) = \varphi(y) <=> e^x = e^y <=> x = y,$$

($\forall$ r $\in$ R^+) ($\exists$ x $\in$ R): φ(x) = y, а именно, x = ln y, т.к. $\varphi(\ln y) = e^{\ln y} = y$

и сохраняет групповую операцию:

$$(\forall x, y \in R) \quad \varphi(x + y) = e^{x+y} = e^x \bullet e^y = \varphi(x) \bullet \varphi(y).$$

Задания

1. Выяснить, образует ли кольцо относительно обычных сложения и умножения множество натуральных чисел.

2. Выяснить, является ли $\langle M,+,\cdot\rangle$ кольцом, если $M = \{a + b\sqrt{3} \mid a,b \in Z\}$.

3. Определить, является ли $\langle Z,*,\circ\rangle$ кольцом, полем, если $(\forall a,b \in Z)$ $a * b = a + b + 1, a \circ b = ab + a + b$.

4. Гомоморфны ли алгебры $\langle Z,+\rangle$ и $\langle 2Z,+\rangle$, если задано отображение $\varphi: Z \to 2Z$ по следующему правилу: $(\forall x \in Z)\,\varphi(x) = 2x$? Является ли φ изоморфизмом?

5. Выяснить, является ли $\varphi:\langle Z^+,+\rangle \to \langle Z,\cdot\rangle$ изоморфизмом, если $\varphi(x) = 7x$.

6. Выяснить, является ли φ гомоморфизмом (изоморфизмом), если: $\varphi:\langle Z,*,\circ\rangle \to \langle Z,+,\cdot\rangle, \varphi(a) = a + 5, a * b = a + b + 5, a \circ b = ab + 5a + 5b + 20$;

$\varphi:\langle Z,+,\cdot\rangle \to \langle Z,+,\cdot\rangle, \varphi(a) = 0$.

7. Верно ли, что…а) множество с заданной на нём бинарной операцией – это группоид; б) моноид – это группоид, в котором существует нейтральный элемент; в) группа – это моноид, в котором для каждого элемента существует обратный?

8. Выяснить, какой алгебраической структурой является $\langle R \setminus \{0\},*\rangle$, если $a * b = 5ab \ \ \forall a,b \in R \setminus \{0\}$.

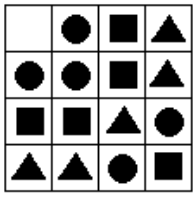
9. Определить, является ли $\langle A,+\rangle, A = \{12^k \mid k \in N \cup \{0\}\}$, подгруппой аддитивной группы целых чисел.

10. Определить, является ли $\langle M,+\rangle$ подгруппой аддитивной группы действительных чисел, если $M = \{a + b\sqrt{5} \mid a,b \in Q\}$.

11. Определить, будет ли мультипликативная алгебра положительных действительных чисел подгруппой аддитивной группы действительных чисел.

12. Составить кластер понятий по теме «Группа» и обосновать его.

13. (Задачао наследовании признака). Пусть имеется конечное множество *M* простейших существ, каждое из которых обладает одним из признаков *A, B, C*. Пусть, например, эти признаки характеризуют форму глаз: соответственно круглые, квадратные и треугольные. Известно, что в результате слияния двух существ *X* и *Y* получается одно новое существо *Z*. При этом наследование формы глаз осуществляется по закону «*» описанному таблицей на рисунке:

14. 

15. В результате эволюции существ остается одно существо. Доказать, что форма глаз оставшегося существа не зависит от того, в каком порядке сливаются существа.

16. К кубику Рубика применили последовательность поворотов. Доказать, что применяя ее несколько раз, можно привести кубик в начальное состояние.

17. Доказать, что множество всех наборов фиксированной длины *n,* составленных из 0 и 1, образует аддитивную группу по операции суммирования по модулю два. Что представляет собой элемент, противоположный произвольному элементу а этой группы?

18. Восстановить цепочку понятий между понятиями «отображение» и «изоморфизм групп», в которой каждое следующее понятие образуется из предыдущего через видовое отличие.

19. Построить левое и правое разбиения группы симметрий правильного треугольника на смежные классы: а) по подгруппе вращений этого треугольника; б) по подгруппе $A=\{R_0,a\}$, где *а* – одна из симметрий.

20. Построить левое и правое разложения мультипликативной группы действительных чисел на смежные классы по подгруппе $A=\{-1;1\}$.

21. Построить таблицу Кэли для группы симметрий квадрата.

22. Построить фактор-группу аддитивной группы целых чисел по ее подгруппе целых чисел, кратных пяти. Построить таблицу Кэли для этой группы и найти элемент, противоположный элементу 2+B.

23. Дано множество $F=\{f_1; f_2; f_3; f_4\}$, где $f_1(x)=x,\ f_2(x)=-x,\ f_3(x)=\frac{1}{x},\ \ f_4(x)=-\frac{1}{x}$. Выяснить, образует ли данное множество группу по операции композиции функций. Если да, то найти все подгруппы этой группы и построить разбиение на смежные классы по какой-либо подгруппе.

24. Определить, образует ли группу по операции умножения множество классов вычетов, взаимно простых с модулем m=8.

Тема. Теория делимости в кольце целых чисел и кольце многочленов

План

1. Деление целых чисел с остатком. НОД и НОК целых чисел. Алгоритм Евклида.

2. Деление с остатком. Деление многочлена на двучлен. Корни многочлена.

3. Алгоритм Евклида для многочленов

1. Деление целых чисел с остатком. НОД и НОК целых чисел. Алгоритм Евклида

Задание 1. Найти с помощью расширенного алгоритма Евклида числа x и y для a=1250, b=675.

Решение.

Из примера 1 получили, что НОД (1250, 675) = 25.

Запишем шаги алгоритма Евклида в виде равенств:

$$a = 1250 = 675\cdot 1 + 575 = r_0,$$

$$b = 675 = 575\cdot 1 + 100 = r_1,$$

$$575 = 100\cdot 5 + 75 = r_2,$$

$$100 = 75\cdot 1 + 25 = d.$$

Выразим теперь из каждого равенства остаток и подставим его в последующее равенство

$$575 = a - b,$$
$$100 = b - 575 \Rightarrow 100 = b - (a - b),$$
$$75 = 575 - 100\cdot 5 \Rightarrow 75 = (a - b) - [b - (a - b)]\cdot 5,$$
$$d = 25 = 100 - 75 \Rightarrow d = [b - (a - b)] - \{(a - b) - [b - (a - b)]\cdot 5\}.$$

В последнем выражении приведем подобные при числах *a* и *b*:

$$d = b - a + b - \{a - b - [5b - 5a + 5b]\} =$$
$$= 2b - a - a + b + 5b - 5a + 5b =$$
$$= 13b - 7a.$$
$$НОД\ (1250, 675) = -7\cdot 1250 + 13\cdot 675 \Rightarrow x = -7,\ y = 13.$$

Задание 2. Простым или составным является число 1267?

Решение.

Пользуясь признаками делимости на 2, 3 и 5, можно утверждать, что ни на одно из этих простых чисел данное число не делится. Число 1267 также не делится на 11, 13, 17, 19, 23, 29, 31. Делимость на последующие простые числа, по свойству 1, проверять нет необходимости, так как $\sqrt{1267} > 37^2 = 1369$.

Поэтому число 1267 является простым.

Задание 3. Найти НОД и НОК чисел 1250 и 675 разложением на простые множители.

Решение.

Так как $1250 = 2\cdot 5^4$, а $675 = 3^3\cdot 5^2$, то

$$НОД\ (1250, 675) = 5^2 = 25;$$
$$НОК\ (1250, 675) = 2\cdot 3^3\cdot 5^4 = 33750.$$

Задания

1. Дано $a = b + c$. а) $a \vdots d, b \vdots d$. Следует ли из этого, что $c \vdots d$? б) $a \vdots d$. Верно ли, что $b \vdots d$ и $c \vdots d$?
2. Дано $a \vdots b$. Выяснить, верно ли, что $(\forall n \in N)\ a \vdots bn$.
3. Выполнить деление с остатком: 168 на 35; 168 на (-35); -168 на 35; -168 на (-35).
4. Найти делители и соответствующие им остатки, если: а)делимое 534, частное 26; б) делимое 741, частное (-14).
5. Доказать, что квадрат любого целого числа либо нацело делится на 3, либо дает в остатке 1.
6. Числа a, b, c при делении на 7 дают остатки 1, 4, 5 соответственно. Найти остаток от деления числа $a + b + c$ на 7.
7. Найти все числа, большие 25000, но меньшие 30000, у которых как при делении на 131, так и при делении на 1965 остаток равен 125.
8. Найти НОД и НОК чисел 531 и 93; -78 и 24.
9. Найти НОД(663, 731, 2516, 3655).
10. Решить в натуральных числах следующие системы уравнений:

а) $\begin{cases} x + y = 180, \\ (x; y) = 30; \end{cases}$ б) $\begin{cases} (x; y) = 4, \\ x \cdot y = 720; \end{cases}$ в) $\begin{cases} (a; b) = 15, \\ [a; b] = 420. \end{cases}$

11. Найти линейное представление НОД (90; 35) через эти числа.
12. Пусть a, b, c, d – различные цифры. Доказать, что число cdcdcdcd не делится на число aabb.`
13. Число при некоторой перестановке своих цифр удваивается. Доказать, что оно делится на 9.

14. Найти натуральные числа, дающие при делении на 2, 3, 4, 5 и 6 остаток 1 и, кроме того, делящиеся на 7.

15. Генерал построил солдат в колонну по 4, но при этом солдат Иванов остался лишним. Тогда генерал построил солдат в колонну по 5. И снова Иванов остался лишним. Когда же и в колонне по 6 Иванов оказался лишним, генерал посулил ему наряд вне очереди, после чего в колонне по 7 Иванов нашел себе место и никого лишнего не осталось. Сколько солдат могло быть у генерала?

16. Доказать, что если НОК(a, a+5)=НОК(b, b+5), где a и b – натуральные числа, то a = b.

17. Пусть d = НОД(1819, 3587). Найти d и целые числа x, y такие, что: 1819x+3587y=d .

2. Деление с остатком. Деление многочлена на двучлен. Корни многочлена

Задание 1. Даны многочлены

$$F_4(x)=6-5x+4x^2-3x^3+2x^4,$$

$$Q_2(x)=1-3x+x^2.$$

Используя определение, найти $F_4(x)Q_2(x)$.

Решение.

Так как $\deg[F(x)Q(x)]=\deg F(x)+\deg Q(x)$, то степень произведения $\deg[F(x)Q(x)]=\deg T(x)=6$.

Ищем многочлен вида $T_6(x)=d_0+d_1x+d_2x^2+d_3x^3+d_4x^4+d_5x^5+d_6x^6$, где коэффициенты вычисляем по общей формуле $d_k=\sum_{i+j=k}a_ia_j\ \ (k=0,1,2,\ldots,6)$.

Подставляя данные $a_0=6$, $a_1=-5$, $a_2=4$, $a_3=-3$, $a_4=2$, $b_0=1$, $b_1=-3$ $b_2=1$ в эту формулу, получаем:

$$d_0=a_0b_0=6;$$

$$d_1=a_0b_1+a_1b_0=-18-5=-23;$$

$$d_2=a_0b_2+a_1b_1+a_2b_0=6+(-5)\cdot(-3)+4\cdot1=25;$$

$$d_3=a_1b_2+a_2b_1+a_3b_0=(-5)\cdot1+4\cdot(-3)+(-3)\cdot1=-20;$$

$$d_4=a_2b_2+a_3b_1+a_4b_0=4\cdot1+(-3)\cdot(-3)+2\cdot1=15;$$

$$d_5=a_3b_2+a_4b_1=(-3)\cdot1+2\cdot(-3)=-9;$$

$$d_6=a_4b_2=2.$$

Следовательно, искомый многочлен имеет вид $T_6(x)=6-23x+25x^2-20x^3+15x^4-9x^5+2x^6$. $\otimes$

Задание 2. Выполнить деление с остатком многочлена:

$F_4(x)=3x^4+4x^3+x^2-x-18$ на многочлен $G_2(x)=x^2+3x+2$.

Решение.

Воспользуемся общим алгоритмом согласно которому имеем деления многочленов с остатком:

1) $F_3^{(1)}(x)=F_4(x)-\frac{a_4}{b_2}x^{4-2}G_2(x)=3x^4+4x^3+x^2-x-18-$

$-3x^2(x^2+3x+2)=-5x^3-5x^2-x-18;$

2) $F_2^{(2)}(x)=F_3^{(1)}(x)-\frac{a_3^{(1)}}{b_2}x^{3-2}G_2(x)=-5x^3-5x^2-x-18+$

$+5x(x^2+3x+2)=10x^2+9x-18;$

3) $F_1^{(3)}(x)=F_2^{(2)}(x)-\frac{a_2^{(2)}}{b_2}x^{2-2}G_2(x)=10x^2+9x-18-$

$-10(x^2+3x+2)=-21x-38$.

Имеем:

$3x^4+4x^3+x^2-x-18=(x^2+3x+2)(3x^2-5x+10)-21x-38$.

Задание 3. Вычислить значение $F(c)$ многочлена $F(x)=x^4-8x^3+24x^2-50x+22$, если $c=2$.

Решение.

По теореме Безу значение многочлена $F(c)$ равно остатку от деления многочлена $F(x)$ на линейный двучлен $x-c$. Поэтому, деля многочлен $F(x)$ на $x-2$, получаем:

$$\begin{array}{l|l} F(x)=x^4-8x^3+24x^2-50x+22 & \\ \underline{-(x^4-2x^3)} & \\ -6x^3+24x^2-50x+22 & \dfrac{x-2}{x^3-6x^2+12x-26} \\ \underline{-(-6x^3+12x^2)} & \\ 12x^2-50x+22 & \\ \underline{-(12x^2-24x)} & \\ -26x+22 & \\ \underline{-(-26x+52)} & \\ -30 & \end{array}$$

Итак, $F(c)=-30$.

Задание 4. При каких условиях многочлен $F(x)$ делится на многочлен $G(x)$, если $F(x)=x^3+px+q$, $G(x)=x^2+mx-1$.

Решение.

Пусть для определённости, $F(x)\in C[x]$ и $G(x)\in C[x]$. Тогда по определению делимости многочленов имеем:

$F(x)\vdots G(x)\Leftrightarrow(\exists\Phi(x)\in C[x])\colon F(x)=G(x)\cdot\Phi(x)$.

Для нахождения многочлена $\Phi[x]$ производим деление «уголком»:

$$\begin{array}{l|l} F(x)=x^3+px+q & \dfrac{G(x)=x^2+mx-1}{\Phi(x)=x-m} \\ \underline{-(x^3+mx^2-x)} & \\ -mx^2+(p+1)x+q & \\ \underline{-(-mx^2-m^2x+m)} & \\ R(x)=(p+m^2+1)x+q-m & \end{array}$$

Чтобы выполнялось равенство $F(x)=G(x)\cdot\Phi(x)$, то есть

$F(x)=x^3+px+q=(x^2+mx-1)(x-m)$,

должно быть $R(x)=(p+m^2+1)x+q-m=0$, откуда, приравнивая коэффициенты к нулю, получаем искомые условия: $p=-1-m^2$, $q=m$.

Задание 5. Найти НОД$(F(x),G(x))$, если $F(x)=x^4+4x^3-7x+2$, $G(x)=x^3+3x^2-4$.

Решение.

Используем общую схему алгоритма Евклида

1) Делим $F(x)$ на $G(x)$ с остатком:

$$\begin{array}{l|l} F(x)=x^4+4x^3-7x+2 & \\ \underline{x^4+3x^3-4x} & \dfrac{G(x)=x^3+3x^2-4}{Q_1=x+1} \\ x^3-3x+2 & \\ \underline{x^3+3x^2-4} & \\ R_1(x)=-3x^2-3x+6 & \end{array}$$

2) Делим $G(x)$ на $R_1(x)$ с остатком:

$$\begin{array}{l|l} G(x)=x^3+3x^2-4 & \\ \underline{x^3+x^2-2x} & \dfrac{R_1(x)=-3x^2-3x+6}{Q_2=-\dfrac{1}{3}x-\dfrac{2}{3}} \\ 2x^2+2x-4 & \\ \underline{2x^2+2x-4} & \\ 0 & \end{array}$$

Получаем наибольший общий делитель данных многочленов в виде $(F(x), G(x))=R_1(x)=-3x^2-3x+6$, или по неоднозначности определения НОД $(F(x), G(x))=x^2+x-2$.

Задание 6. Найти многочлен $F(x)=a_0+a_1x+a_2x^2$, если $F(1)=1, F(2)=2, F(3)=3$.

Решение.

Для нахождения многочлена требуется определить его коэффициенты a_0, a_1, a_2. Из условия задачи для коэффициентов имеем систему линейных алгебраических уравнений

$$\begin{cases} a_0+a_1+a_2=1, \\ a_0+2\,a_1+4\,a_2=2, \\ a_0+3\,a_1+9\,a_2=3. \end{cases}$$

Решаем СЛАУ методом Гаусса. Для этого совершаем ряд последовательных исключений.

1) Из первого уравнения $a_0=1-a_1-a_2$ подставляем во второе:

$$\begin{cases} a_0+a_1+a_2=1, \\ a_1+3\,a_2=1, \\ a_0+3\,a_1+9\,a_2=3. \end{cases}$$

2) Из второго уравнения $a_1=1-3a_2$ подставляя в третье:

$$\begin{cases} a_0+a_1+a_2=1, \\ a_1+3\,a_2=1, \\ 2\,a_2=0. \end{cases}$$

Двигаемся «обратным ходом» (находимся в поле действительных чисел):

3) из третьего уравнения находим $a_2=0$;

4) из второго уравнения находим $a_1=1$;

5) из первого уравнения находим $a_0=0$.

Составляем многочлен

$F(x)=a_0+a_1x+a_2x^2=x$.

Проверка очевидна. Искомый многочлен имеет вид $F(x)=x$.

Задание 7. Разложить многочлен $f(x)=x^3+1$ на неприводимые множители над полями R и C.

Решение.

$x^3+1=(x+1)(x^2+x+1)$ (1) Над R: Многочлен x^2+x+1 не имеет действительных корней, следовательно (1) и есть разложение над полем R.

Над C: $x^2+x+1=0,\ D=-3=3i,\ i^2=-1,\Rightarrow x_{1,2}=\dfrac{-1\pm i\sqrt{3}}{2}$. Тогда искомое разложение на полем C будет иметь вид: $x^3+1=(x+1)\left(x-\dfrac{-1-i\sqrt{3}}{2}\right)\left(x+\dfrac{-1-i\sqrt{3}}{2}\right)$.

Задание 8. Разделить с остатком многочлен f(x)=x^3-4x^2+3x+5 на многочлен g(x)=x^2-3x+1.

Решение.

$$\begin{array}{r|l} x^3-4x^2+3x+5 & x^2-3x+1 \\ \hline x^3-3x^2+x & x-1 \\ \hline -x^2+2x+5 & \\ -x^2+3x-1 & \\ \hline -x+6 & \end{array}$$

Ответ: $x^3-4x^2+3x+5=(x-1)(x^2-3x+1)+(-x+6)$.

Задание 9. Разделить многочлен f(x) = x^3+2x-5 на двучлен x – 2 с помощью схемы Горнера.

Решение.

В данном случае c = 2.

	1	0	2	-5
c = 2	1	0 + 2·1 = 2	2 + 22 = 6	-5 + 2·6 = 7

Итак, x^3+2x-5 = $(x-2)\cdot(x^2+2x+6)+7$, следовательно, значение многочлена f(x) при x = 2 равно, согласно теореме 1, семи: f(2) = 7.

Задание 10. Разложить многочлен f(x) = x^3+2x-5 по степеням разности x – 2.

Решение.

По схеме Горнера выполним ряд последовательных делений с остатком на x – 2:

	1	0	2	-5
c = 2	1	0 + 2·1 = 2	2 + 2·2 = 6	-5 + 2·6 = 7
c = 2	1	4	14	
c = 2	1	6		
c = 2	1			

Таким образом, беря в качестве коэффициентов последние члены в каждой строке полученной схемы, можно записать:

$$x^3+2x-5 = (x-2)^3+6\cdot(x-2)^2+14\cdot(x-2)+7.$$

Задание 11. Найти значения производных многочлена f(x) = x^3+2x-5 при x = 2.

Решение.

Из схемы Горнера, построенной в примере 3, получаем:

$b_0 = \dfrac{f(2)}{0!} = 7, \quad \Rightarrow \quad f(2) = 7\cdot 0! = 71 = 7,$

$b_1 = \dfrac{f'(2)}{1!} = 14, \quad \Rightarrow \quad f'(2) = 14\cdot 1! = 14,$

$$b_2 = \frac{f''(2)}{2!} = 6, \quad \Rightarrow \quad f''(2) = 6\cdot 2! = 6\cdot 2 = 12,$$

$$b_3 = \frac{f^{(3)}(2)}{3!} = 1, \quad \Rightarrow \quad f^{(3)} = 1\cdot 3! = 1\cdot 6 = 6,$$

Так как все последующие коэффициенты $b_4, b_5, \ldots, b_k,$ равны нулю, то и значения всех производных данного многочлена, начиная с производной четвертого порядка, также будут равны нулю.

Задание 12. Разложить на множители многочлен над полем $\mathbb{Q}$

$$f(x) = x^4 - 15x^3 + 69x^2 - 72x - 108.$$

Решение.

Возможные целые корни — делители 108: $\pm 1, \pm 2, \pm 3, \pm 4, \pm 6, \pm 9, \pm 12, \pm 27, \pm 36, \pm 54, \pm 108$.

Пусть α— целый корень, $f(\alpha) = 0$.

$$f(x) = (x-\alpha)g(x),$$
$$f(1) = 1 - 15 + 69 - 72 - 108 = -125,$$
$$f(1) = (1-\alpha)g(1),$$
$$f(1) \vdots (\alpha - 1).$$

Из последней делимости следует, что корень нужно искать среди чисел 2; –4 и 6. Проверим их с помощью схемы Горнера:

	1	-15	69	-72	-108
2	1	-13	43	14	-80
-4	1	-19	119	590	$\neq 0$
6	1	-9	15	18	0
6	1	-3	-3	0	

Числа 2 и –4 не являются корнями многочлена, число 2 – является. Поэтому

$$f(x) = (x-6)^2(x^2 - 3x - 3).$$

Задания

1. Записать в стандартном виде сумму и разность многочленов $f(x) = 2x^6 - 8x^3 + 3x^5 - 35x - 18 + 17x^2$ и $g(x) = 5x^5 - 2x^4 - 2x^6 + 10x^3 + 35x + 8$.

2. Записать в стандартном виде произведение многочленов $f(x) = 3x^4 - 2x^3 + 2x^2 + 7$ и $g(x) = 5x^3 + 4x - 5$.

3. Проверить, что в кольце $Z[x]$ многочлен $f(x) = 6x^3 + 11x^2 - 13x + 2$ делится на многочлен $g(x) = 2x^2 + 5x - 1$ (двумя способами).

4. Разделить с остатком $f(x) = x^4 - 4x^3 + 5x^2 + x - 1$ на $g(x) = x^2 - 2x - 3$.

5. Найти многочлен $f(x) = a_0 + a_1x + a_2x^2$, если $f(1) = 1, f(2) = 2, f(3) = 3$.

6. Известны делимое $f(x) = 2x^4 + x^3 + 3x^2 + 1$, неполное частное $q(x) = 2x^2 + 3x + 2$ и остаток $r(x) = -4x - 3$. Найти делитель $g(x)$.

7. Пусть $f(x) \in Z[x]$. При каких p, q многочлен $f(x) = x^4 + px^2 + q$ делится на $g(x) = x^2 + x + 1$?

8. Многочлен $P(x)$ делится без остатка на $(x-1)$ и $(x+1)$, а при делении на $(x+3)$ даёт в остатке 8. Найти остаток от деления $P(x)$ на $x^3 + 3x^2 - x - 3$.

9. Доказать, что при любом натуральном n и $a \in A$ (A – область целостности): а) $(x^n - a^n) \vdots (x-a)$; б) $(x^{2n} - a^{2n}) \vdots (x+a)$.

10. Составить кубический многочлен, корнями которого являются числа 2, 4 и (-1), а старший коэффициент равен 4.

11. Пользуясь схемой Горнера, разделить с остатком многочлен $f(x)=x^6+4x^5-5x^4+3x^3-4x^2+2x-1$ на двучлен $(x-2)$.

12. Найти показатель кратности корня $x_0=-2$ для многочлена $f(x)=x^5+7x^4+16x^3+8x^2-16x-16$.

13. Разложить многочлен $f(x)=x^4-6x^3+12x^2-26x+37$ по степеням двучлена $(x-2)$.

14. Найти значение многочлена $f(x)=2x^5+7x^4-x^3+3x-2$ и всех его производных при $x=-3$ и разложить $f(x)$ по степеням двучлена $(x+3)$.

15. Вычислить значения многочлена $f(x)=x^4+5x^3-9x^2+7$ при $x=3{,}01$ и $x=2{,}98$.

3. Алгоритм Евклида для многочленов

Задание 1. Найти $НОД(f,g)$ для $f=x^2-1$ и $g=x+1$ над R.

Решение.

Многочлен f делится на все многочлены вида $\lambda(x^2-1)$, $\lambda\in R$, $(\lambda\neq 0)$, на все многочлены вида $\beta(x-1)$, $\beta\in R$, $(\beta\neq 0)$, на все многочлены вида $\gamma(x+1)$, $\gamma\in R$, $(\gamma\neq 0)$, на все многочлены вида μ, $\mu\in R$, $(\mu\neq 0)$. Многочлен g делится на все многочлены вида $\delta(x+1)$, $\delta\in R$, $(\delta\neq 0)$, и на все многочлены вида ω, $\omega\in R$, $(\omega\neq 0)$. Общими делителями многочленов f и g являются все многочлены вида $a(x+1)$, $a\in R$, $(a\neq 0)$ и все многочлены вида c, $c\in R$, $(c\neq 0)$. Среди них делятся на все общие делители многочленов f и g только многочлены вида $a(x+1)$, $a\in R$, $(a\neq 0)$. Значит, они и являются общими делителями многочленов f и g. Их бесконечно много. Среди них выделяется нормированный $НОД(f,g)=x+1$.

$НОД(f,g)$ можно найти с помощью алгоритма Евклида.

Пусть даны $f\neq\bar{0}$ и $g\neq\bar{0}$ и $\deg f\geq\deg g$.

1)Разделим f на g: $f=g\cdot q_1+r_1$, $\deg r_1<\deg g$,

2)Если $r_1\neq\bar{0}$, то разделим g на r_1: $g=r_1\cdot q_2+r_2$, $\deg r_2<\deg r_1$,

3)Если $r_2\neq\bar{0}$, то разделим r_1 на r_2: $g_1=r_2\cdot q_3+r_3$, $\deg r_3<\deg r_2$, и т.д. до тех пор, пока в остатке не получится $\bar{0}$:

$$r_{k-2}=r_{k-1}\cdot q_k+r_k,\qquad \deg r_k<\deg r_{k-1},\qquad r_k\neq\bar{0}.$$

$$r_{k-1}=r_k\cdot q_{k+1}+\bar{0}.$$

$$НОД(f,g)=r_k.$$

Заметим, что деление нужно производить «уголком».

Задание 2. Найти $НОД(f,g)$, если $f=2x^3-3x^2+x-5$, $g=x^2-2x+1$.

Решение.

1) $f=g\cdot q_1+r_1$,
$q_1=2x+1$, $r_1=x-6$

$$\begin{array}{r|l} 2x^3-3x^2+x-5 & x^2-2x+1 \\ \hline \bar{}\,2x^3-4x^2+2x & 2x+1 \\ \hline x^2-x-5 & \\ \bar{}\,x^2-2x+1 & \\ \hline x-6 & \end{array}$$

2) $g = r_1 \cdot q_2 + r_2,$
$q_2 = x + 4,\ r_2 = 25$

$$\begin{array}{r|l} x^2 - 2x + 1 & x - 6 \\ \hline \bar{}\,x^2 - 6x & x + 4 \\ \hline 4x + 1 & \\ \bar{}\,4x - 24 & \\ \hline 25 & \end{array}$$

3) $r_1 = r_2 \cdot q_3 + r_3,$
$q_3 = 1/25\,x - 6/25,\ r_3 = \bar{0}$

$$\begin{array}{r|l} x - 6 & 25 \\ \hline \bar{}\,x & 1/25\,x - 6/25 \\ \hline -6 & \\ -6 & \\ \hline 0 & \end{array}$$

Значит, $НОД(f, g) = 25$. Запишем нормированный $НОД(f, g)$: $d = 1$.

С помощью алгоритма Евклида для многочленов f и g всегда можно подобрать такие m_1 и m_2, что $f \cdot m_1 + g \cdot m_2 = НОД(f, g)$.

Задание 3. Для многочленов f и g подобрать такие многочлены m_1 и m_2, чтобы $f \cdot m_1 + g \cdot m_2 = НОД(f, g)$, если алгоритм Евклида для f и g состоит из двух строк.

Решение.

Пусть алгоритм Евклида для многочленов f и g состоит из двух строк:

$$f = g \cdot q_1 + r_1,$$
$$g = r_1 \cdot q_2 + \bar{0}.$$

Тогда $НОД(f, g) = r_1$.

Выделим r_1 из первой строки алгоритма: $r_1 = f - g \cdot q_1 = f \cdot 1 + g(-q_1)$. Тогда $m_1 = 1,\ m_2 = -q_1$.

Задание 4. Выделить кратные неприводимые множители многочлена

$$f = x^8 - x^6 - 2x^5 + 2x^3 + x^2 - 1 \in R[x].$$

Решение.

Дифференцируя f, получаем $f' = 8x^7 - 6x^5 - 10x^4 + 6x^2 + 2x$.

С помощью алгоритма Евклида находим

$$НОД(f, f') = x^4 - x^3 - x + 1 = (x^3 - 1) \cdot (x - 1) = (x^2 + x + 1) \cdot (x - 1)^2.$$

Отсюда следует, что кратными неприводимыми множителями многочлена f являются многочлены $p_1 = x^2 + x + 1$ (кратности 2) и $p_2 = x - 1$ (кратности 3).

Разделив f на $(x^2 + x + x)^2 (x - 1)^3$ получим $p_3 = x + 1$.

Итак, $f = (x^2 + x + 1)^2 (x - 1)^3 (x + 1)$.

Так как корни многочлена соответствуют его неприводимым множителям первой степени, то корни многочлена $НОД(f, f')$– это кратные корни многочлена f. Поэтому выделение кратных неприводимых множителей является в то же время выделением кратных корней многочлена f.

Задания

1. Найти НОД многочленов $f(x)=3x^5+6x^4+3x^3-x^2-2x-1$ и $g(x)=x^4-2x^2+1$. (Ответ: x^2+2x+1)

2. Найти линейное выражение НОД многочленов через сами эти многочлены: $f(x)=2x^4+3x^3-3x^2-5x+2$, $g(x)=2x^3+x^2-x-1$.

3. Разложить многочлен $f(x)=x^2+\sqrt{2}$ на неприводимые множители над полем R; над полем C.

4. Разложить многочлены на неприводимые множители над полем действительных чисел: а) a^5-a^2-a-1; б) x^8+x^4-2; в) $y^{12}-3y^6+1$.

5. Разложить многочлен $f(x)=x^4+1$ на неприводимые множители над полями C, R, Q.

6. Найти НОД многочлена $f(x)=(x+1)\cdot(x^4-1)\cdot(x^3-1)$ и его производной.

7. Найти $НОД(f,g)$, если $f=(x-1)^2\cdot(x^2-1)^3$ и $g=(x+1)^2\times.\times(x-2)$

8. Для многочленов f и g подобрать такие многочлены m_1 и m_2, чтобы $f\cdot m_1+g\cdot m_2=НОД(f,g)$, если алгоритм Евклида для f и g состоит из трех строк.

9. Выделить кратные неприводимые множители многочлена $f=x^8-x^6-2x^5+2x^3+x^2-1\in R[x]$.

10. Отделить кратные множители многочлена $f(x)=x^6-6x^4-4x^3+9x^2+12x+4$.

Тема. Расширения полей. Конечные поля

План

1. Понятие расширения поля. Минимальный многочлен алгебраического числа и его свойства.

2. Поля Галуа. Представление элементов поля Галуа конечными числовыми последовательностями и многочленами над конечным полем.

1. Понятие расширения поля. Минимальный многочлен алгебраического числа и его свойства

Задание 1. Описать строение поля K=Q(α), где Q – поле рациональных чисел: $\alpha=\sqrt{7+\sqrt{2}}$.

Решение.

Построим минимальный многочлен числа α над полем рациональных чисел:

$$x=\sqrt{7+\sqrt{2}}\Rightarrow x^2=\left(\sqrt{7+\sqrt{2}}\right)^2\Rightarrow$$

$$x^2=7+\sqrt{2}\Rightarrow x^2-7=\sqrt{2}\Rightarrow\left(x^2-7\right)^2=\left(\sqrt{2}\right)^2\Rightarrow$$

$$x^4-14x+49=2\Leftrightarrow x^4-14x+47=0.$$

Число $\alpha=\sqrt{7+\sqrt{2}}$ будет корнем многочлена $p(x)=x^4-14x+47$ по построению, причём очевидно, что степень этого многочлена минимальна и равна $n=4$.

Следовательно, базис простого алгебраического расширения K=Q(α)над полем рациональных чисел также состоит из четырёх элементов:

$$\alpha^0=1,\ \alpha,\ \alpha^2,\ \alpha^3.$$

Так как $\alpha=\sqrt{7+\sqrt{2}}$, то базис примет вид:

$$1,\ \sqrt{7+\sqrt{2}},\ \left(\sqrt{7+\sqrt{2}}\right)^2,\ \left(\sqrt{7+\sqrt{2}}\right)^3\ \Leftrightarrow$$

$$1,\ \sqrt{7+\sqrt{2}},\ 7+\sqrt{2},\ \left(\sqrt{7+\sqrt{2}}\right)^3.$$

Тогда произвольный элемент поля K=Q(α) будет иметь вид:

$$\forall \omega \in Q\left(\sqrt{7+\sqrt{2}}\right)\ \ \omega = a_0 + a_1 \cdot \sqrt{7+\sqrt{2}} + a_2 \cdot \left(7+\sqrt{2}\right) + a_3 \cdot \left(\sqrt{7+\sqrt{2}}\right)^3,\ a_i \in Q,\ i = \overline{0,3}.$$

Задание 2. Избавиться от иррациональности в знаменателе дроби

$$\frac{\alpha^4+\alpha^2+2}{\alpha^2+2},\ \text{где}\ \alpha^3+\alpha-1=0.$$

Решение.

Пусть $\alpha^4+\alpha^2+2 = f(\alpha);\ \alpha^2+2 = g(\alpha)$, тогда $f(x) = x^4+x^2+2,\ g(x) = x^2+2$

Нетрудно проверить, что многочлен $p(x) = x^3+x-1$ не имеет рациональных корней и, значит, неприводим в кольце Q[x]. Так как p(α)=0, то этот многочлен является минимальным для числа α.

Используя замечание, найдем линейное выражение многочлена $f(x)$ через многочлены $g(x)$ и $p(x)$ методом неопределенных коэффициентов.

Из замечания следует, что степень $u(x)$ будет равна 2, а степень $v(x)$ – 1:

$$f(x) = x^4+x^2+2 = (\underbrace{ax^2+bx+c}_{u(x)})g(x) + (\underbrace{dx+k}_{v(x)})p(x) \quad (5).$$

Выполнив действия в правой части равенства и приведя подобные, получим:

$$f(x) = x^4+x^2+2 = (a+d)x^4 + (b+k)x^3 + (2a+c+d)x^2 + (2b-d+k)x + (2c-k).$$

Используя определение равенства двух многочленов, придем к системе линейных уравнений

$$\begin{cases} a+d=1; \\ b+k=0; \\ 2a+c+d=1; \\ 2b-d+k=0; \\ 2c-k=-2. \end{cases}$$

Решив систему, находим: $\begin{cases} a=1; \\ c=-1; \\ b=d=k=0 \end{cases} \Rightarrow u(x) = x^2-1;\ v(x) = 0.$

Поэтому:

$$f(\alpha) = \alpha^4+\alpha^2+2 = (\alpha^2-1)\cdot g(\alpha) + 0 \cdot p(\alpha) = (\alpha^2-1)\cdot g(\alpha) = (\alpha^2-1)\cdot(\alpha^2+2).$$

Подставим в исходное выражение значение, полученное для $\alpha^4+\alpha^2+2$, получим:

$$\frac{\alpha^4+\alpha^2+2}{\alpha^2+2} = \frac{(\alpha^2-1)\cdot(\alpha^2+2)}{\alpha^2+2} = \alpha^2-1.$$

Задание 3. Пусть P=Q($\sqrt{2},\sqrt{3}$) – конечное расширение поля рациональных чисел. Найти число γ, такое, чтобы Q($\sqrt{2},\sqrt{3}$) = Q(γ).

Решение.

Будем искать число γ в виде:

$\gamma = \sqrt{2} + c\sqrt{3}$, где c – подходящее число из поля Q, (2).

Число *c* выберем следующим образом. Пусть $p_1(x)$ и $p_2(x)$ - минимальные многочлены чисел $\sqrt{2}$ и $\sqrt{3}$ соответственно:

$$p_1(x) = x^2-2,\ p_2(x) = x^2-3 \quad (3).$$

Из (2) следует, что $\sqrt{2}$ = γ - c$\sqrt{3}$ (4).

Рассмотрим многочлен

$$q(x) = p_1(\gamma - cx) \quad (5),$$

коэффициенты которого принадлежат полю Q(γ). Очевидно, что $\sqrt{3}$ является корнем этого многочлена, так как

$$q(\sqrt{3}) = p_1(\gamma - c\sqrt{3}) = p_1(\sqrt{2}) = 0.$$

С другой стороны, $\sqrt{3}$ есть корень $p_2(x)$, коэффициенты которого принадлежат полю Q, а следовательно, и полю Q(γ). Потребуем, чтобы многочлены q(x) и $p_2(x)$ не имели других общих корней, кроме числа $\sqrt{3}$.

Так как многочлен $p_2(x)$ имеет только два корня: $\sqrt{3}$ и - $\sqrt{3}$, то - $\sqrt{3}$ может быть общим корнем $p_2(x)$ и q(x), только если число

$$\gamma - c\cdot(-\sqrt{3})$$

будет корнем многочлена $p_1(x)$, то есть, если

$$\gamma - c\cdot(-\sqrt{3}) = \sqrt{2} \quad (7) \text{ или } \gamma - c\cdot(-\sqrt{3}) = -\sqrt{2} \quad (7')$$

Поэтому, чтобы многочлены q(x) и $p_2(x)$ не имели других общих корней, кроме $\sqrt{3}$, достаточно потребовать, чтобы

$$c \neq \frac{\pm\sqrt{2} - \sqrt{2}}{2\sqrt{3}},$$

т.е., чтобы $c \neq 0$ и $c \neq -\frac{\sqrt{2}}{\sqrt{3}}$.

Возьмем, например, c = 1. Тогда из равенства (2)

$$\gamma = \sqrt{2} + \sqrt{3} \text{ и } Q(\sqrt{2}, \sqrt{3}) = Q(\sqrt{2} + \sqrt{3}).$$

Из решения этой задачи видно, что, вообще говоря, число γ может быть выбрано неоднозначно.

2. Поля Галуа. Представление элементов поля Галуа конечными числовыми последовательностями и многочленами над конечным полем

Задание 1. Построить поле Галуа GF(3).

Решение.

Здесь $q = 3$. Все элементы поля Галуа являются корнями многочлена $f(x) = x^3 - x = x(x^2 - 1)$. Корни многочлена $f(x)$ равны $x_1 = 0,\ x_2 = 1,\ x_3 = -1$.

Поэтому $GF(3) = \{0, 1, =1\}$. Зададим сложение и умножение так, чтобы на множестве GF(3) были групповыми операциями:

$$\begin{array}{cccc} + & 0 & 1 & -1 \\ 0 & 0 & 1 & -1 \\ 1 & 1 & 0 & 0 \\ -1 & -1 & 0 & 0 \end{array} \qquad \begin{array}{ccc} \bullet & 1 & -1 \\ 1 & 1 & -1 \\ -1 & -1 & 1 \end{array}.$$

Получили $< GF(3), +, \bullet >$ – поле Галуа.

Задание 2. Построить поле GF(4) как расширение поля GF(2) по модулю многочлена $p(x)=x^2 + x+1$.

Решение.

Представим элементы поля в виде последовательностей длины 2 (двумерные векторы) и как многочлены степени 1 и меньше и зададим их в виде таблицы:

Последовательность длины 2	Многочлен
00	0
10	1
01	α
11	$1+\alpha$

Правила сложения и умножения в этом поле приведены на рисунке:

а)

+	0	1	α	α^2
0	0	1	α	α^2
1	1	0	α^2	α
α	α	α^2	0	1
α^2	α^2	α	1	0

б)

·	0	1	α	α^2
0	0	0	0	0
1	0	1	α	α^2
α	0	α	α^2	1
α^2	0	α^2	1	α

Рис. П.1.5

Задания

1. Найти значения всех элементов поля как расширение: а) GF(2) по неприводимому многочлену $p(x)=x^3+x+1$; б) GF(3) по неприводимому многочлену $p(x) = x^3+x+2$.
2. Найти циклические порождающие полей GF(4) и GF(9).
3. Найти все неприводимые многочлены степени два над полем GF(5).
4. Решить в поле GF(7) уравнения $x^4 = 3$ и $x^2 + x + 1 = 0$.
5. Избавиться от иррациональности в знаменателе выражения $\frac{5}{1-\sqrt[4]{2}+\sqrt{2}}$.
6. Избавиться от иррациональности в знаменателе выражения $\frac{\alpha^2-3\alpha-1}{\alpha^2+2\alpha+1}$, $\alpha^3+\alpha^2+3\alpha+4=0$;
7. Описать строение поля $K=Q(\alpha)$, где Q – поле рациональных чисел и найти элемент, обратный для элемента β: $\alpha=\sqrt{7+\sqrt[3]{3}}$, $\beta=\sqrt[3]{3}-\sqrt{7+\sqrt[3]{3}}$.

Тема. Элементы теории кодирования

План

1. Представление об алфавитном кодировании.
2. Сжатие. Простейшие алгоритмы сжатия.
3. Помехоустойчивые коды как пример оптимальных кодов.

1. Представление об алфавитном кодировании

Пусть дано множество $A=\{a_1, a_2, \ldots, a_n\}$, состоящее из n элементов. Множество А будем называть *алфавитом объема n,* а его элементы - *символами* или *буквами* алфавита. Конечную последовательность символов алфавита будем называть *словом* в этом алфавите, а количество символов в слове – его *длиной.*

Любое непустое множество слов, записанное в алфавите А, называется *кодом* в этом алфавите. Мощность этого множества слов называется *объемом кода,* а элементы этого множества – *кодовыми словами.*

Код называется *равномерным,* Если все его кодовые слова имеют одинаковую длину m. В этом случае m называется *длиной равномерного кода.*

Рассмотрим на конкретных примерах некоторые способы кодирования слов русского языка.

Подстановочные шифры

В русском алфавите отождествим буквы «е» и «ё», а также буквы «ъ» и «ь». Получим алфавит из 31 буквы. Добавим к ним новый, 32 –й символ, означающий

промежуток между словами. Если теперь рассмотреть инъективное отображение преобразованного вышеуказанным образом русского алфавита в произвольное множество M мощности ≥ 32, а затем заменить в некотором тексте каждую букву на ее образ из множества M, то получится набор слов в алфавите M, который называется *подстановочной криптограммой*.

Чтобы расшифровать подобную криптограмму, требуется знать относительную частоту появления той или иной буквы русского алфавита в произвольном тексте. Это можно сделать следующим образом: взять достаточно объемный текст (например, роман Л.Н. Толстого «Война и мир») и подсчитать частоту вхождения в него каждой буквы. Результаты можно свести в таблицу:

Таким способом, например, знаменитый сыщик Шерлок Холмс расшифровал таинственное послание в романе А. Конан Дойла «Пляшущие человечки» (с той разницей, что он, конечно составлял подобную таблицу для букв английского алфавита).

Довольно известным примером подстановочного шифра является так называемый *шифр Цезаря*. Он состоит в том, что для кодировки символов какого-либо алфавита (например, русского) вместо каждого символа подставляется символ этого же алфавита, предшествующий данному (или следующий за ним) на несколько позиций.

Задание 1. Рассмотрим шифр Цезаря со сдвигом на две позиции вниз применительно к русскому алфавиту, т.е.:

$$а \to ю,\ б \to я,\ в \to а,\ г \to б \text{ и т.д. (1)}$$

и закодируем с его помощью фразу:

ЖИЗНЬ БЕЗ МАТЕМАТИКИ НЕВЫНОСИМО СКУЧНА.

Решение.

Используя правило (1), получим следующую фразу:

ДЖЕЛЩ ЯГЕ КЮРГКЮРЖИЖ ЛГАШЛМПКМ ПИСХЛЮ.

Для того, чтобы облегчить расшифровку текста, закодированного шифром Цезаря, применяется «метод полосок». Каждая полоска состоит из выписанных вертикально подряд букв русского алфавита. Для расшифровки, например, слова «ДЖЕЛЩ» берутся пять таких полосок и прикладываются друг к другу так, чтобы получилось это слово. Тогда ниже этого слова можно будет прочитать его расшифровку.

Перестановочные шифры

Самый простой способ использования перестановочного шифра заключается в том, что каждой букве русского алфавита сопоставляется ее номер от 1 до 31 согласно таблице 1, а пробелу между словами – номер 32. Полученную последовательность чисел рассматривают в кольце Z_{32} классов вычетов по mod 32. Затем в этом кольце выбирается произвольный обратимый элемент $\overline{p}$ и каждый член последовательности умножается на p. Если полученное при умножении число превосходит 32, то оно заменяется на соответствующее число по mod 32, которое в свою очередь заменяется буквой русского алфавита по таблице 1.

Чтобы расшифровать полученное сообщение, необходимо снова переписать его в виде последовательности чисел, умножить каждое из чисел на элемент, обратный $\overline{p}$ в кольце Z_{32}, и наконец, заменить новую последовательность чисел буквами по таблице 1.

Задание 2. Закодировать сообщение:

ЭКЗАМЕН ПО ИНФОРМАТИКЕ УСПЕШНО СДАН.

Решение.

Первый способ

Заменяя буквы на их порядковые номера в русском алфавите, получим последовательность чисел:

29, 11, 8, 1, 13, 6, 14, 32, 16, 15, 32, 9, 14, 21, 15, 17, 13, 1, 19, 9, 11, 6, 32, 18, 5, 1, 14, 32, 20, 18, 16, 6, 25, 14, 15. (*)

В качестве обратимого элемента кольца Z_{32} возьмем, например, вычет $\bar{3}$:

$$\bar{3}\cdot\overline{11}=\overline{11}\cdot\bar{3}$$

и умножим на 3 все числа последовательности (*):

23, 1, 24, 3, 7, 18, 10, 32, 16, 13, 32, 27, 10, 31, 13, 19, 7, 3, 25, 27, 1, 18, 32, 22, 15, 3, 10, 32, 28, 22, 16, 18, 11, 10, 13. (**)

Заменим числа последовательности (**) буквами по таблице 1:

«ЩАЧВЖСЙ ПМ ЫЙЯМТЖВШЫАС ХОВЙ ЪХПСКЙМ».

Чтобы расшифровать эту фразу, вернемся к последовательности (**) и умножим каждое ее число на элемент, обратный к $\bar{3}$, который равен $\overline{11}$:

29, 11, 8, 1, 13, 6, 14, 32, 16, 15, 32, 9, 14, 21, 15, 17, 13, 1, 19, 9, 11, 6, 32, 18, 5, 1, 14, 32, 20, 18, 16, 6, 25, 14, 15,

т.е. получили последовательность (*), заменяя числа которой соответствующими буквами по таблице 1, получим исходную фразу.

Второй способ.

Более сложный способ использования перестановочного шифра заключается в использовании невырожденных матриц над кольцом Z_{32}.

Полученную последовательность чисел (*) разобьем на пары. Так как в этой последовательности нечетное количество чисел, то добавим в конце последовательности пробел, который кодируется числом 32:

$$\begin{pmatrix}29\\11\end{pmatrix},\begin{pmatrix}8\\1\end{pmatrix},\begin{pmatrix}13\\6\end{pmatrix},\begin{pmatrix}14\\32\end{pmatrix},\begin{pmatrix}16\\15\end{pmatrix},\begin{pmatrix}32\\9\end{pmatrix},\begin{pmatrix}14\\21\end{pmatrix},\begin{pmatrix}15\\17\end{pmatrix},\begin{pmatrix}13\\1\end{pmatrix},\begin{pmatrix}19\\9\end{pmatrix},\begin{pmatrix}11\\6\end{pmatrix},\begin{pmatrix}32\\18\end{pmatrix},\begin{pmatrix}5\\1\end{pmatrix},\begin{pmatrix}14\\32\end{pmatrix},$$
$$\begin{pmatrix}20\\18\end{pmatrix},\begin{pmatrix}16\\6\end{pmatrix},\begin{pmatrix}25\\14\end{pmatrix},\begin{pmatrix}15\\32\end{pmatrix}. \qquad (***)$$

Умножим любую обратимую квадратную матрицу второго порядка, на каждую из полученных одностолбцовых матриц, например, это может быть матрица

$$A=\begin{pmatrix}2 & 7\\ -3 & 6\end{pmatrix}\in M_2(Z_{32}),$$

обратной для которой будет матрица

$$A^{-1}=\begin{pmatrix}6 & -7\\ 3 & 2\end{pmatrix}\in M_2(Z_{32}).$$

После умножения получим новую последовательность столбцов:

$$\begin{pmatrix}7\\11\end{pmatrix},\begin{pmatrix}23\\14\end{pmatrix},\begin{pmatrix}4\\29\end{pmatrix},\begin{pmatrix}28\\22\end{pmatrix},\begin{pmatrix}9\\10\end{pmatrix},\begin{pmatrix}31\\22\end{pmatrix},\begin{pmatrix}15\\20\end{pmatrix},\begin{pmatrix}21\\25\end{pmatrix},\begin{pmatrix}1\\31\end{pmatrix},\begin{pmatrix}5\\29\end{pmatrix},\begin{pmatrix}32\\3\end{pmatrix},\begin{pmatrix}30\\12\end{pmatrix},\begin{pmatrix}17\\23\end{pmatrix},\begin{pmatrix}28\\22\end{pmatrix},$$
$$\begin{pmatrix}6\\16\end{pmatrix},\begin{pmatrix}10\\20\end{pmatrix},\begin{pmatrix}20\\23\end{pmatrix},\begin{pmatrix}30\\19\end{pmatrix}. \qquad (****)$$

Заменяя каждое число буквой по табл. 1, получим закодированную информацию в виде фразы:

ЖЙЦНГЭЪХИЙЯХОУФШАЯДЭ 32 ЛРЦЪХЕПЙУЦЮТ.

Чтобы расшифровать эту фразу, нужно вместо букв подставить в нее их номера и разбить на пары. Получится последовательность столбцов (****). Умножая матрицу A^{-1} на каждый столбец из этой последовательности и заменяя вновь полученные номера соответствующими буквами, восстановим исходную фразу. Естественно, что для использования этого способа необходимо знать матрицу А.

Задание 3. Закодировать фразу:

ЖИЗНЬ СТУДЕНТА ПОЛНА ОПАСНОСТЕЙ

с использованием ключевого слова.

Можно считать этот способ кодирования третьим способом.

Решение.

В качестве ключевого слова может быть использовано любое слово, в котором буквы не повторяются, например, слово ДЕКАН.

Весь текст вместе с ключевым словом поместим в таблицу:

Д	***Е***	***К***	***А***	***Н***
2	***3***	***4***	***1***	***5***
Ж	***И***	***З***	***Н***	***Ь***
С	***Т***	***У***	***Д***	***Е***
Н	***Т***	***А***	***П***	***О***
Л	***Н***	***А***	***О***	***П***
А	***С***	***Н***	***О***	***С***
Т	***Е***	***Й***		

Числа, записанные ниже ключевого слова, означают порядок следования букв этого слова в алфавите. Чтобы закодировать нашу фразу с помощью таблицы 2, будем выписывать из нее буквы в следующем порядке: сначала все буквы, записанные (сверху вниз) в столбце под номером 1. затем в столбце под номером 2 и т.д.:

НДПООЖСНЛАТИТТНСЕЗУААНЙЬЕОПС. (1)

Для декодирования полученной фразы нужно знать либо ключевое слово, либо число 23415.

Если число букв в закодированной фразе нацело делится на число букв ключевого слова, то строим таблицу соответствующей размерности и заполняем ее буквами (начиная с последней в фразе и двигаясь к ее началу): сначала столбец с самым большим номером и далее по убыванию. Если же число букв фразы не делится нацело на число букв ключевого слова, то берем самое близкое к нему число, которое уже делится на него нацело и строим таблицу.

Например, в нашем случае число букв ключевого слова равно 5, а всей фразы – 28. Поэтому берем число 30 и строим таблицу размерности 5×6, в которой две последние ячейки будут лишними.

Задание 4. Закодировать шифром Тритемиуса фразу:

КАЖДЫЙ ДОЛЖЕН УМЕТЬ СЧИТАТЬ.

Решение.

Шифр Тритемиуса также основан на использовании ключевого слова. Кодируемую фразу записывают подряд без пробелов. Под ней записывают также без пробелов ключевое слово столько раз, сколько оно уместится (буквы ключевого слова не должны повторяться). Затем заменяют буквы верхнего и нижнего ряда числами по таблице 1 и складывают верхнее число с нижним, приводя результат по mod 31. Полученную последовательность чисел заменяют соответствующими буквами. Получается закодированная фраза.

В качестве ключевого слова возьмем слово «ЛОГИКА».

Записываем под нашей фразой ключевое слово:

КАЖДЫЙДОЛЖЕНУМЕТЬСЧИТАТЬ

ЛОГИК АЛОГИКАЛОГИКАЛОГИКАЛО

Заменим буквы в верхнем и нижнем ряду их номерами, после чего, складывая числа первой и второй строк и приводя результат по mod 31, получим:

2, 16, 11, 14, 7, 11, 17, 30, 16, 16, 17, 15, 1, 28, 10, 28, 8, 19, 5, 24, 23, 10, 30, 29.

Заменяем каждое число буквой:

БПКНЖКРЮППРОАЪЙЪЗТДЧЦЙЮЭ (2).

Чтобы расшифровать полученную фразу, нужно знать запись ключевого слова в кольце Z_{31} (в нашем случае – 12, 15, 4, 9, 11, 1), перейти от закодированного текста (2)

к числовой записи и вычесть из каждого числа (по mod 31) номер соответствующей ключевой буквы.

Задание 4. Закодировать слово «ИНСТИТУТ» табличным способом.

Решение.

Рассмотрим произвольное инъективное отображение φ русского алфавита в множество $N \times N$. Кодирование слов заключается в замене каждой буквы ее образом – то есть некоторой парой натуральных чисел. Отображение φ удобно задавать в виде таблицы. Пусть отображение φ задано таблицей 3 (6×6):

	1	***2***	***3***	***4***	***5***	***6***
1	***а***	***о***	***н***	***л***	***м***	***к***
2	***п***	***б***				***й***
3	***р***	***я***	***в***	***щ***		***и***
4	***с***	***ю***	***ы***	***г***	***ш***	***з***
5	***т***	***э***	***ь***	***ч***	***д***	***ж***
6	***у***	***ф***	***х***	***ц***		***е***

Тогда слову «ИНСТИТУТ» соответствует набор упорядоченных пар:

<3, 6>; <1, 3>; <4, 1>; <5, 1>; <3, 6>; <5, 1>; <6, 1>; <5, 1>

или число 36 13 41 51 36 51 61 51.

Зная таблицу, по данному числу исходное слово декодируется однозначно.

Рассмотренные способы алфавитного кодирования являются простыми. Естественно, ими не исчерпываются все способы алфавитного кодирования. Существуют достаточно сложные способы, требующие знания теории сравнений и других разделов абстрактной алгебры.

2. Сжатие. Простейшие алгоритмы сжатия

Задание 1. Сжать методом Шеннона-Фано файл состоит из некоторой символьной строки: *aaaaaaaaaabbbbbbbbccccccddddeeeefff.*

Решение.

Каждый символ этой строки можно закодировать, как показано в таблице 1.

Таблица 1. Пример построения кода Шеннона-Фано

Символ	**Частота появления**	**Код**
a	10	11
b	8	10
c	6	011
d	5	010
e	4	001
f	3	000

Итак, если обычно каждый символ кодировался 7—8 битами, то теперь требуется максимум 3 бита.

Задание 2. Закодировать методом Хаффмена символьную строку, у которой частота появления символов задана таблицей 2.

Решение.

Таблица2. Кодирование методом Хаффмена.

Символ	Частота появления	Вспомогательные столбцы						
c	22	22	22	26	32	42	58	100
e	20	20	20	22	26	32	42	
h	16	16	16	20	22	26		
l	16	16	16	16	20			
a	10	10	16	16				
k	10	10	10					
m	4	6						
b	2							

Более наглядно принцип действия метода Хаффмена можно представить В виде кодового дерева (рис. 1) на основе табл. 2.

Из точки, соответствующей сумме всех вероятностей (в данном случае она равна 100), направляются две ветви. Ветви с большей вероятностью присваивается единица, с меньшей — нуль. Продолжая последовательно разветвлять дерево, доходим до вероятности каждого символа.

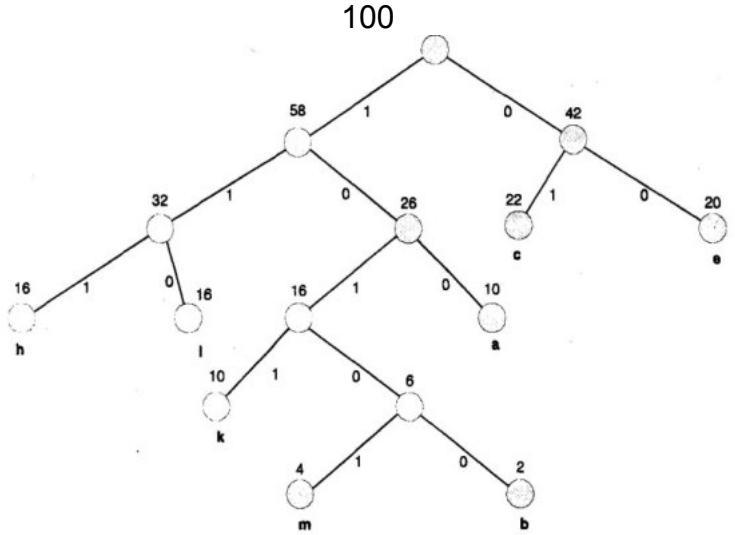


Рис.1. Кодовое дерево для кода Хаффмена

Теперь, двигаясь по кодовому дереву сверху вниз, можем записать для каждого символа соответствующий код (табл. 3).

Таблица 3. Коды символов для кодового дерева.

Символ	Код
c	01
e	00
h	111
l	110
a	100
k	1011
m	10101
b	10100

Задание 3. Определить частоты появления букв, построить кодовое дерево и код Хаффмена, найти среднюю длину кодовых слов для поговорки:

ЧЕТЫРЕ ЧЕРТЕНКА ЧЕРТИЛИ ЧЕРНЫМИ ЧЕРНИЛАМИ ЧЕРТЕЖ.

Решение.

Всего в этой фразе 43 буквы, подсчитаем частоту появления каждой из них, и результат запишем в таблицу 4.

Таблица 4. Построение кода Хаффмена.

Буква	Частота	Вспомогательные столбцы										
Е	9	9	9	9	9	9	9	11	14	18	25	43
Ч	6	6	6	6	6	8	9	9	11	14	18	
Р	6	6	6	6	6	6	8	9	9	11		
И	5	5	5	5	5	6	6	8	9			
Т	4	4	4	4	5	5	6	6				
Н	3	3	4	4	4	5	5					
Ы	2	2	3	4	4	4						
А	2	2	2	3	4							
Л	2	2	2	2								
М	2	2	2									
К	1	2										
Ж	1											
∑	43											

Вспомогательные столбцы получаются следующим образом:

- сначала складываем частоты появления букв «К» и «Ж», и суммарную частоту записываем в первом вспомогательном столбце вместе с остальными частотами (в порядке убывания сверху вниз);
- снова складываем две последние в полученном вспомогательном столбце частоты и записываем во второй вспомогательный столбец также в порядке убывания (в строке буквы «Н» появилась цифра 4) и т.д.

Если все действия выполнены правильно, то в последнем вспомогательном столбце получится число, равное общему количеству букв в поговорке (в данном случае – 43).

Теперь можно строить кодовое дерево. Из точки, соответствующей сумме всех частот (в данном случае она равна 43), направляются две ветви. Ветви с большей частотой присваивается единица, с меньшей — нуль. Продолжая последовательно разветвлять дерево, доходим до частоты появления каждой буквы (рис. 2).

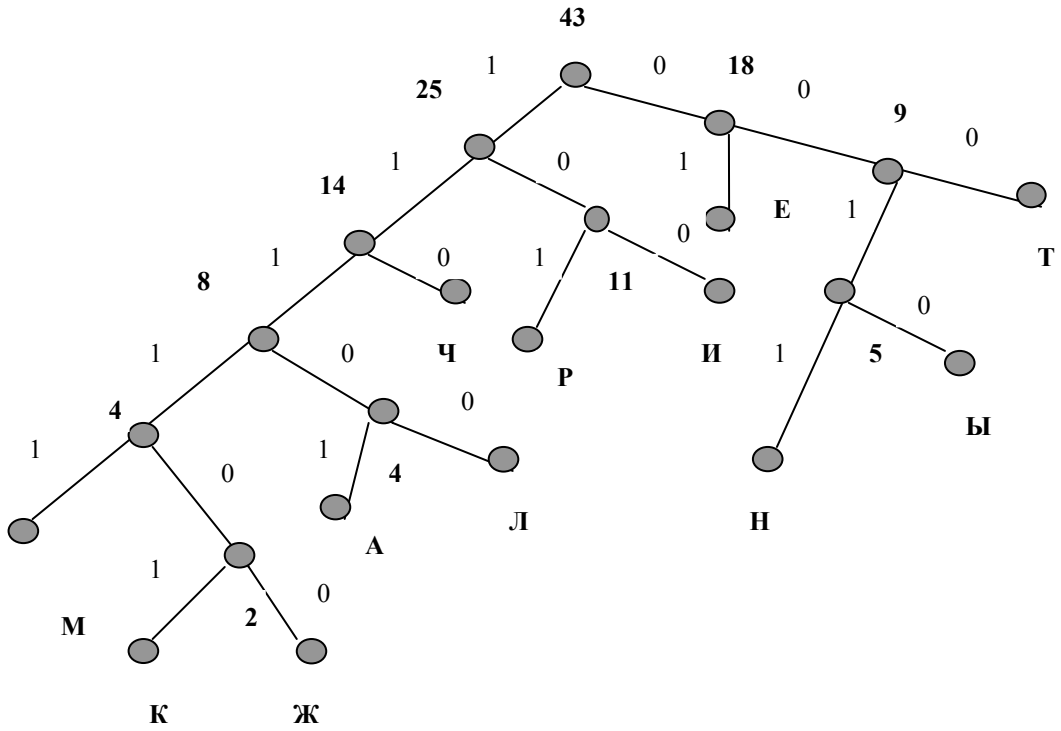


Рис. 2. Кодовое дерево для фразы «Четыре чертенка чертили черными чернилами чертеж».

По кодовому дереву строим код Хаффмена для нашей поговорки, который запишем в таблицу 6.5

Таблица 5. Код Хаффмена для фразы «Четыре чертенка чертили черными чернилами чертеж».

Буква	Код
Е	01
Ч	110
Р	101
И	100
Т	000
Н	0011
Ы	0010
А	11101
Л	11100
М	11111
К	111101
Ж	111100

Подсчитаем среднюю длину кодовых слов как среднее арифметическое длин всех кодовых слов из таблицы 5:

$$l_{ср} = \frac{2 + 4 \cdot 3 + 2 \cdot 4 + 3 \cdot 5 + 2 \cdot 6}{12} = \frac{49}{12} \approx 4,08 .$$

Задания

1. Зашифровать, используя: а) шифр Цезаря со сдвигом вниз на 2 позиции; б) кольцо классов вычетов по mod32; в) ключевое слово из 6 букв; г) шифр Тритемиуса с ключевым словом из задания в), фразу *Человеку не хватает мудрости успокоиться на достигнутом.*

2. Построить для фразы *Забота об излишнем часто соединяется с потерей необходимого* код Шеннона-Фано.

3. Зашифровать текст, используя подстановочные шифры:

Чтоб мудро жизнь прожить, знать надобно немало,
Два важных правила запомни для начала:
Ты лучше голодай, чем что попало есть,
И лучше будь один, чем вместе с кем попало.

4. Построить код Шеннона-Фано для фразы *Кукушка кукушонку купила капюшон, как в капюшоне кукушонок смешон.*

5. Определить частоты появления букв в поговорке, построить кодовое дерево и код Хаффмена, найти среднюю длину кодовых слов для фразы *Два щенка щека к щеке грызли щетку в уголке*.

3. Помехоустойчивые коды как пример оптимальных кодов

Пример 1. В таблице 1 представлены все кодовые слова (5,3)-кода (a_i – информационные; b_i - проверочные символы).

Таблица 1. Кодовые слова (5,3)-кода.

№ п/п	a_1	a_2	a_3	b_1	b_2
1	0	0	1	1	0
2	0	1	0	1	1
3	0	1	1	0	1
4	1	0	0	0	1

5	1	0	1	1	1
6	1	1	0	1	0
7	1	1	1	0	0
8	0	0	0	0	0

Пример 2. Для (5,3)-кода проверочные уравнения имеют вид:

$$b_1 = a_2 + a_3;$$
$$b_2 = a_1 + a_2.$$

Пример 3. (5,3)-код, который был представлен в таблице 1, может быть задан порождающей матрицей:

$$G_{(5,3)} = \begin{vmatrix} 1 & 0 & 0 & 0 & 1 \\ 1 & 0 & 1 & 1 & 1 \\ 1 & 1 & 0 & 1 & 0 \end{vmatrix}.$$

Пример 4. Порождающая матрица для (5,3)-кода в систематическом виде:

$$G_{(5,3)} = \begin{vmatrix} 1 & 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 1 & 1 \\ 0 & 0 & 1 & 1 & 0 \end{vmatrix}.$$

Пример 5. Проверочная матрица (5,3) – кода:

$$H_{(5,3)} = \begin{vmatrix} 0 & 1 & 1 & 1 & 0 \\ 1 & 1 & 0 & 0 & 1 \end{vmatrix}.$$

Пример 6. Для кода (5,3)

$$[10111] \cdot \begin{vmatrix} 0 & 1 \\ 1 & 1 \\ 1 & 0 \\ 1 & 0 \\ 0 & 1 \end{vmatrix} = [00].$$

Пример 7. Для кода (5, 3):

$$H_{(5,3)} = \begin{vmatrix} 0 & 1 & 1 & 1 & 0 \\ \underline{1} & 1 & 0 & 0 & \underline{1} \end{vmatrix}, \quad d_0 = 2;$$

для кода (5, 2):

$$H_{(5,2)} = \begin{vmatrix} 1 & 1 & 1 & 0 & 0 \\ 1 & 0 & 0 & 1 & 0 \\ \underline{1} & \underline{1} & 0 & \underline{0} & 1 \end{vmatrix}, \quad d_0 = 3.$$

Пример 8. Для кода (5, 3):

$$[110] \cdot \begin{vmatrix} 1 & 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 1 & 1 \\ 0 & 0 & 1 & 1 & 0 \end{vmatrix} = [11010].$$

Задание 1. Найти его стандартное расположение (5, 2)-кода, заданного матрицами:

$$G_{(5,2)} = \begin{vmatrix} 1 & 0 & 1 & 1 & 1 \\ 0 & 1 & 1 & 0 & 1 \end{vmatrix} \quad H_{(5,2)} = \begin{vmatrix} 1 & 1 & 1 & 0 & 0 \\ 1 & 0 & 0 & 1 & 0 \\ 1 & 1 & 0 & 0 & 1 \end{vmatrix},$$

Решение.

Всего существует 32 слова длины 5, состоящих из 0 и 1, которые образуют абелеву группу относительно сложения по mod 2. Из них кодовыми являются для (5, 2) кода $2^k = 2^2 = 4$ слова:

$$v_0 = 00000,\ v_1 = 10111,\ v_2 = 01101,\ v_3 = 11010.$$

Нетрудно проверить, что эти слова образуют относительно сложения по mod2 подгруппу в группе всех слов длины 5 (табл. 6).

Таблица 6. Подгруппа кодовых слов (5, 2)-кода.

+ mod2	$\boldsymbol{v}_0$	$\boldsymbol{v}_1$	$\boldsymbol{v}_2$	$\boldsymbol{v}_3$
$\boldsymbol{v}_0$	$\boldsymbol{v}_0$	$\boldsymbol{v}_1$	$\boldsymbol{v}_2$	$\boldsymbol{v}_3$
$\boldsymbol{v}_1$	$\boldsymbol{v}_1$	$\boldsymbol{v}_0$	$\boldsymbol{v}_3$	$\boldsymbol{v}_2$
$\boldsymbol{v}_2$	$\boldsymbol{v}_2$	$\boldsymbol{v}_3$	$\boldsymbol{v}_0$	$\boldsymbol{v}_1$
$\boldsymbol{v}_3$	$\boldsymbol{v}_3$	$\boldsymbol{v}_2$	$\boldsymbol{v}_1$	$\boldsymbol{v}_0$

Например, $v_1 + v_1 = 10111 + 10111 = 00000 = v_0$, $v_2 + v_3 = 01101 + 11010 = 0111 = v_1$ и т.д. Причем, так как группа всех слов длины 5 абелева, то подгруппа кодовых слов будет являться в ней нормальным делителем. Поэтому можно разложить группу всех слов длины 5 на смежные классы по подгруппе кодовых слов.

По теореме Лагранжа, индекс этой подгруппы будет равен 32:4 = 8, т.е. смежных классов будет 8, в каждом по 4 элемента (слова). Соответствующее разложение приведено в таблице 7.

Таблица 7. Стандартное расположение (5, 2)-кода.

$v_0 = 00000$	$v_1 = 10111$	$v_2 = 01101$	$v_3 = 11010$
$l_1 = 00001$	$l_1 + v_1 = 10110$	$l_1 + v_2 = 01100$	$l_1 + v_3 = 11011$
$l_2 = 00010$	$l_2 + v_1 = 10101$	$l_2 + v_2 = 01111$	$l_2 + v_3 = 11000$
$l_3 = 00100$	$l_3 + v_1 = 10011$	$l_3 + v_2 = 01001$	$l_3 + v_3 = 11110$
$l_4 = 01000$	$l_4 + v_1 = 11111$	$l_4 + v_2 = 00101$	$l_4 + v_3 = 10010$
$l_5 = 10000$	$l_5 + v_1 = 00111$	$l_5 + v_2 = 11101$	$l_5 + v_3 = 01010$
$l_6 = 00011$	$l_6 + v_1 = 10100$	$l_6 + v_2 = 01110$	$l_6 + v_3 = 11001$
$l_7 = 10001$	$l_7 + v_1 = 00110$	$l_7 + v_2 = 11100$	$l_7 + v_3 = 01011$

Этот код имеет $d_0 = 3$. Он гарантирует исправление одиночных ошибок, конфигурация которых дана в первом столбце.

Процедура исправления ошибок следующая. Принятое кодовое слово анализируют и определяют, в каком столбце оно находится, в качестве исправленного кодового слова берут слово, находящееся в верхней строке. Однако, если длина кода большая, пользоваться таким алгоритмом неудобно. Поэтому при декодировании используют таблицу синдромов (декодирования), представляющую собой список образцов ошибок (см. первый столбец стандартного расположения) и список соответствующих синдромов.

Задание 2. Построить таблицы декодирования для линейного группового кода, имеющего поверочную матрицу:

$$H = \begin{pmatrix} 1 & 1 & 1 & 0 & 0 \\ 1 & 0 & 0 & 1 & 0 \\ 1 & 1 & 0 & 0 & 1 \end{pmatrix}$$

Решение.

В данном случае n = 5, k = 3, $\Rightarrow$ r = n – k = 2. Поэтому мы имеем групповой 5, 2) – код. В табл. 4 представлен список образцов ошибок (l_1,…, l_7).Найдем для каждой ошибки соответствующий синдром:

$$S_1 = l_1 \cdot H^T = (00001) \cdot \begin{pmatrix} 1 & 1 & 1 \\ 1 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} = (001); \quad S_4 = l_4 \cdot H^T = (01000) \cdot \begin{pmatrix} 1 & 1 & 1 \\ 1 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} = (101);$$

$$S_2 = l_2 \cdot H^T = (00010) \cdot \begin{pmatrix} 1 & 1 & 1 \\ 1 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} = (010); \quad S_5 = l_5 \cdot H^T = (10000) \cdot \begin{pmatrix} 1 & 1 & 1 \\ 1 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} = (111);$$

$$S_3 = l_3 \cdot H^T = (00100) \cdot \begin{pmatrix} 1 & 1 & 1 \\ 1 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} = (100); \quad S_6 = l_6 \cdot H^T = (00011) \cdot \begin{pmatrix} 1 & 1 & 1 \\ 1 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} = (011);$$

$$S_7 = l_7 \cdot H^T = (10001) \cdot \begin{pmatrix} 1 & 1 & 1 \\ 1 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} = (110).$$

Так как S_1= (001), то переводя эту запись в десятичную систему счисления, получим число 1, что означает ошибку в первой позиции. Для S_4 = (101) аналогично получим: 101_2 = 5, т.е. ошибка совершена в пятой позиции, и т.д. На основании полученных данных строим таблицу декодирования:

Таблица 8. Таблица декодирования.

Список образцов ошибок	Синдром	№ позиции с ошибкой
l_1 = 00001	001	№ 1
l_2 = 00010	010	№ 2
l_3 = 00100	100	№ 4
l_4 = 01000	101	№ 5
l_5 = 10000	111	№ 7
l_6 = 00011	011	№ 3
l_7 = 10001	110	№ 6

Пример 9. Для (7,4)-кода Хэмминга проверочная матрица в упорядоченном виде имеет вид:

$$H_{(7,4)} = \begin{vmatrix} 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 1 & 0 & 1 & 0 & 1 & 0 & 1 \end{vmatrix}.$$

Пусть переданное кодовое слово - $v(1,0) = 1101001$, а принятое слово – $v'(1,0) = 1101101$.

Синдром, соответствующий принятому слову будет равен:

$$S(1,0) = v'(1,0) \cdot H^T_{(7,4)} = [1101101] \cdot \begin{vmatrix} 0 & 0 & 1 \\ 0 & 1 & 0 \\ 0 & 1 & 1 \\ 1 & 0 & 0 \\ 1 & 0 & 1 \\ 1 & 1 & 0 \\ 1 & 1 & 1 \end{vmatrix} = [101].$$

Вычисленный синдром указывает на ошибку в пятой позиции.

Проверочная матрица в упорядоченном виде представляет совокупность проверочных уравнений, в которых проверочные символы занимают позиции с номерами 2^i (i=0,1,2...).

Для (7,4)-кода Хэмминга проверочными уравнениями будут:

$$v_1 = v_3 + v_5 + v_7;$$
$$v_2 = v_3 + v_6 + v_7;$$
$$v_4 = v_5 + v_6 + v_7,$$

где v_1, v_2, v_4 - проверочные символы.

Элементы синдрома определяются из выражений:

$$S_0 = v_1 + v_3 + v_5 + v_7;$$
$$S_1 = v_2 + v_3 + v_6 + v_7;$$
$$S_2 = v_4 + v_5 + v_6 + v_7.$$

Корректирующая способность кода Хэмминга может быть увеличена введением дополнительной проверки на четность. В этом случае проверочная матрица для рассмотренного (7,4)-кода будет иметь вид:

$$H_{(8,4)} = \begin{vmatrix} 0 & 0 & 0 & 1 & 1 & 1 & 1 & 0 \\ 0 & 1 & 1 & 0 & 0 & 1 & 1 & 0 \\ 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 \\ 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \end{vmatrix},$$

а кодовое расстояние кода $d_0 = 4$.

Проверочные уравнения используются для построения кодера, а синдромные - декодера кода Хэмминга.

Пример 10. Пусть кодовое слово циклического кода имеет вид:

$$\upsilon(1,0) = 1011101001,$$

тогда соответствующий ему многочлен будет равен:

$$\mathcal{M}(x) = x^9 + x^7 + x^6 + x^5 + x^3 + 1.$$

Например, если код построен над полем GF(q)=GF(2^3), которое является расширением поля GF(2) по модулю неприводимого многочлена $f(z)=z^3+z+1$, а элементы этого поля имеют вид, представленный в таблице 9.

Таблица 9. Элементы поля GF(2^3).

0	000	0	α^3	011	Z+1
α^0	001	1	α^4	110	Z^2+Z
α^1	010	Z	α^5	111	Z^2+Z+1
α^2	100	Z^2	α^6	101	Z^2+1

то коэффициенты ν_i принимают значения элементов этого поля и поэтому они сами отображаются в виде многочленов следующего вида

$$\mathcal{U}_i(z) = a_{m-1} \cdot z^{m-1} + a_{m-2} \cdot z^{m-2} + \ldots + a_1 \cdot z^1 + a_0 \cdot z^0,$$

где m – степень многочлена, по которому получено расширение поля GF(2); a_i – коэффициенты, принимающие значение элементов GF(2), т.е. 0 и 1.

Такой код называется q-ичным.

Задание 3. Осуществить единичный правый циклический сдвиг кодового слова [1011], используя полиномиальную интерпретацию.

Решение.

Вектору [1011] соответствует многочлен $1 + x^2 + x^3$. Умножим его на x, что дает: $x + x^3 + x^4$. Далее, найдем остаток от деления на $x^n + 1$. В нашем случае n = 4, так как кодовое слово имеет длину 4, поэтому $x^n + 1 = x^4 + 1$:

$$x + x^3 + x^4 \equiv 1 + x + x^3 \pmod{x^4 + 1},$$

поэтому остаток равен: $1 + x + x^3$.

Многочлен $1 + x + x^3$ соответствует вектору [1101], который получается из вектора [1011] правым циклическим сдвигом на одну позицию.

Ответ: [1101].

Пример 11. а) Сумма многочленов:

$$+\begin{array}{r} x^6 + x^4 + x^3 + x + 1 \\ x^3 + x^2 \\ \hline x^6 + x^4 + x^2 + x + 1 \end{array}.$$

Так как в сумме многочленов коэффициент при x^3 оказался равным 2, то приводя его по mod 2, получаем 0.

б) Произведение многочленов:

$$\times x^6 + x^4 + x^3 + x + 1$$
$$\underline{\qquad\qquad x^2 + 1}$$
$$+ x^6 + x^4 + x^3 + x + 1$$
$$\underline{x^8 + x^6 + x^5 + x^3 + x^2}$$
$$x^8 + x^5 + x^4 + x^2 + x + 1 .$$

Аналогично пункту а), в многочлене, равном произведению исходных, не оказалось слагаемых в шестой и третьей степени. Далее, если длина кода равна, например, 7, то результат приводим по mod x^7+1.

$$+ x^8 + x^5 + x^4 + x^2 + x + 1 \quad \big|\underline{x^7 + 1}$$
$$\underline{x^8 + x} \qquad\qquad x$$
$$x^5 + x^4 + x^2 + 1$$

При построении и декодировании циклических кодов в результате деления многочленов обычно необходимо иметь не частное, а остаток от деления. Поэтому рекомендуется более простой способ деления, используя не многочлены, а только его коэффициенты (вариант 2 в примере 4).

Пример 12.

$$+ x^8 + x^5 + x^4 + x^2 + x + 1 \quad \big|\underline{x^5 + x^3 + x + 1}$$
$$\underline{x^8 + x^6 + x^4 + x^3} \qquad\qquad x^3 + x + 1$$
$$+ x^6 + x^5 + x^3 + x^2 + x + 1$$
$$\underline{x^6 + x^4 + x^2 + x}$$
$$+ x^5 + x^4 + x^3 + 1$$
$$\underline{x^5 + x^3 + x + 1}$$
$$x^4 + x \ \ (10010) \ - \textit{остаток}$$

$$+ 100110111$$
$$\underline{101011}$$
$$110111$$
$$+$$
$$\underline{101011}$$
$$111001$$
$$101011$$
$$\underline{\qquad}$$
$$10010 \quad - \textit{остаток}.$$

Задания

1. Найти проверочные уравнения, построить схемы кодирующего и декодирующего устройств для кодов Хэмминга со следующими параметрами (9,5).
2. Найти проверочную матрицу для кода Хэмминга длины 11, обеспечивающего кодовое расстояние равное 4.
3. Построить стандартное расположение кода Хэмминга, кодовые слова которого имеют длину, равную семи.

4. Осуществить единичный правый циклический сдвиг кодового слова [1011], используя полиномиальную интерпретацию.

5. Многочлен $g(x)=x^8+ x^7+ x^6+ x^4+1$ порождает циклический код над GF(2) длины 15. Сколько ошибок и стираний может исправлять код?

6. Найти порождающий многочлен линейного циклического кода длины n=15, который осуществляет кодирование сообщений длины k=7 если дано разложение многочлена $x^{15}+1$ на множители:

7. $x^{15}+1=(1+x)(1+x+x^2)(1+x+x^2+x^3+x^4)(1+x+x^4)(1+x^3+x^4)$,

8. поэтому можно взять $g(x)=(1+x+x^2+x^3+x^4)(1+x+x^4)=1+x^4+x^6+x^7+x^8$. Кодировать сообщение [0110110].

9. Декодировать полученное слово [011010111010010], которое было отправлено после кодирования кодом из предыдущей задачи. Соответствующий вектору [011010111010010] многочлен имеет вид: $x + x^2 + x^4 + x^6 + x^7 + x^8 + x^{10} + x^{13}$

10. Линейный (5, 3)-код над GF(4) имеет порождающую матрицу

$$G_{(5,3)} = \begin{vmatrix} 1 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 & 2 \\ 0 & 0 & 1 & 1 & 3 \end{vmatrix}.$$

а) найти проверочную матрицу;

б) доказать, что этот код исправляет одиночные ошибки.

в) доказать, что этот код исправляет два стирания.

г) составить таблицу кода.

Тематика рефератов/докладов/эссе, методические рекомендации по выполнению контрольных и курсовых работ, иные материалы

Темы докладов (сообщений) по дисциплине Элементы абстрактной и компьютерной алгебры

1 Классификация помехоустойчивых кодов

2 Элементы теории Галуа

3 Описание и принципы работы нормальных алгоритмов Маркова (НАМ)

4 Разбиение множества. Фактор-множество. Классификации.

5. Отношения порядка. Отношения строгого, нестрогого и линейного порядка.

6. Упорядоченные множества.

7. Алгебраические структуры с одной бинарной операцией. Полугруппы.

8. Гомоморфизмы и изоморфизмы групп.

9. Гомоморфизмы и изоморфизмы колец и полей.

10. Различные формы представления комплексных чисел.

11. Операции над комплексными числами в тригонометрической форме.

12. Многочлены от нескольких переменных. Элементарные симметрические многочлены.

13. Формулы Виета для многочлена произвольной степени. Связь элементарных симметрических многочленов с формулами Виета.

14. Из истории алфавитного кодирования.

15. Теоремы Шеннона и роль в развитии теории кодирования.

Разноуровневые задания по дисциплине Элементы абстрактной и компьютерной алгебры

1 Составление глоссария и кластера основных терминов раздела (нескольких разделов) дисциплины (реконструктивный уровень)

2 Составление сравнительных, концептуальных таблиц по заданной теме (творческий уровень)

3 Составление, коррекция синквейнов и денотатных графов с основными понятиями (творческий уровень)

4 Составление аннотированного перечня источников сети Интернет (реконструктивный уровень)

5 Написание рецензий на готовые рефераты по разделам дисциплины, скачанные с различных сайтов (творческий уровень)

6 Составление таблицы толстых и тонких вопросов по разделам дисциплины (реконструктивный уровень)

7 Составление вопросов к ромашке Блума (таксономия целей) к разделам дисциплины (творческий уровень)

Презентации по дисциплине Элементы абстрактной и компьютерной алгебры

1. Бинарные операции и алгебраические структуры
2. Группы, кольца, поля
3. Подгруппы. Порядок элемента группы.
4. Кольца и поля
5. Конечные группы
6. Алфавитное кодирование
7. Простейшие алгоритмы сжатия информации

Материалы для проведения текущей и промежуточной аттестаций представлены в фондах оценочных средств по дисциплине Элементы абстрактной и компьютерной алгебры